

Digitized by the Internet Archive  
in 2024 with funding from  
University of Toronto









Report of the  
Commission  
of Inquiry  
into the  
**CONFIDENTIALITY  
OF HEALTH  
INFORMATION**

Commissioner  
The Hon. Mr. Justice Horace Krever

VOLUME II

Printed by J.C. Thatcher, Queen's Printer for Ontario

ISBN: The Report (3 volumes):0-7743-5567-0

ISBN: Volume 2:0-7743-5569-7

# Table Of Contents

## Volume 1

	Letter of Transmittal	iii
	Orders-in-Council	v
	Preface	ix
<i>Chapter 1</i>	Introduction	1
<i>Chapter 2</i>	Recommendations	13
<i>Chapter 3</i>	Summary of Ontario Legislation	50
<i>Chapter 4</i>	The Physician-Client Relationship	115
<i>Chapter 5</i>	Centurion Investigation Limited	166
<i>Chapter 6</i>	Quest Investigation Limited	291
<i>Chapter 7</i>	Equifax Services Limited	311
<i>Chapter 8</i>	Carl Franco and Franco Investigation Services	345
<i>Chapter 9</i>	Albert George Oxlade and Griffin Investigation Agency	354
<i>Chapter 10</i>	W. A. King Limited and C.C.R.	363



<i>Chapter 11</i>	Cortlaw Services Limited	428
<i>Chapter 12</i>	Jolie & Todd Investigations	437
<i>Chapter 13</i>	State Farm Mutual Automobile Insurance Company	494
<i>Chapter 14</i>	The Automobile Casualty and Liability Insurance Industry in Retrospect	514
<i>Chapter 15</i>	The Lawyers	532

## Volume 2

<i>Chapter 16</i>	The Police and Law Enforcement	1
<i>Chapter 17</i>	The Ontario Health Insurance Plan Computer System	123
<i>Chapter 18</i>	Computer-Supported Systems in Health: The Threat to Privacy	157
<i>Chapter 19</i>	The Hospital Medical Records Institute	192
<i>Chapter 20</i>	The Medical Information Bureau, Inc.	217
<i>Chapter 21</i>	Hospitals and Other Health-Care Institutions	235
<i>Chapter 22</i>	Individual Health-Care Providers	379

<i>Chapter 23</i>	Access to One's Own Health Information	455
<i>Chapter 24</i>	Psychiatric Records and The Advisory Review Board	491

### Volume 3

<i>Chapter 25</i>	Consent to Disclosure	1
<i>Chapter 26</i>	Research	15
<i>Chapter 27</i>	The Unique Personal Health Identifier	53
<i>Chapter 28</i>	Mandatory Reporting of Health Information	73
<i>Chapter 29</i>	Student Health Information	114
<i>Chapter 30</i>	Employee Health Information	152
<i>Chapter 31</i>	Ontario Government Employee Health Information	210
<i>Chapter 32</i>	The Workmen's Compensation Board	232
<i>Chapter 33</i>	The Occupational Health and Safety Act, 1978	267

<i>Appendix I</i>	Common Law Remedies for Disclosure of Confidential Medical Information A Study by Professor S. Rodgers-Magnet	297
<i>Appendix II</i>	Confidentiality Provisions in Ontario Legislation, Part I - Ministry of Health Part II - Other Ministries	368 396
<i>Appendix III</i>	Survey of Health Insurance Systems	432
<i>Appendix IV</i>	Appearances at Hearings	440
<i>Appendix V</i>	List of Briefs	490
<i>Appendix VI</i>	Selected Bibliography	498



## The Police and Law Enforcement

Elsewhere in this report a full description is given of the procedures followed by the Ontario Health Insurance Plan and the manner in which information is received and maintained by the Plan. In order to explain the involvement of the Royal Canadian Mounted Police with OHIP it is necessary to give a less complete outline of the OHIP system at the time of the events discussed in this section and throughout the period of our hearings.

The Ontario Health Insurance Plan, in its present form, was created by The Health Insurance Act, 1972, S.O. 1972, chapter 91. It provides insurance against the cost of certain "insured services" which are defined in the Act as:

...services of hospitals and health facilities as are prescribed by the regulations, all services rendered by physicians that are medically necessary and such other health care services as are rendered by such practitioners and under such conditions and limitations as are prescribed by the regulations...

OHIP maintains relevant medical claims information on the claims reference file which consists of a number of computer tapes. The contents of this claims reference file are reproduced monthly on microfiche, which are film negatives, approximately six inches by four inches each containing 208 computer pages of OHIP information in reduced form. Approximately 7,000 sheets of microfiche comprise one set of the monthly output of the claims reference file. An individual microfiche may be inserted into a viewer and the information contained on the negative is enlarged to readable size. By pushing a button on a special combination printer and viewer a paper reproduction of what is seen on the viewer is made. "Claims fiche" or "medical fiche" as the claims reference file out-put on microfiche is called, are produced monthly and contain all diagnostic and treatment information provided to the Ontario Health Insurance Plan with respect to insured services.

Monthly, sets of claims fiche are shipped, as indicated below, to the various OHIP district offices throughout the Province:

<u>Number of sets shipped</u>	<u>Location of District Office</u>
2	Mississauga
2	Oshawa
1	Ottawa
4	Hamilton
2	London
1	Kingston
1	2195 Yonge Street, Toronto
1	Sudbury
1	Thunder Bay

Many district offices control satellite offices. These district offices sometimes ship the previous month's claims fiche to satellite offices. Prior to the commencement of our hearings, there were no effective controls on distribution or destruction or a consistently implemented destruction policy for these microfiche. The claims fiche contain, in easily readable form, all health information maintained by OHIP about all subscribers and their dependants. The effect of this distribution of the claims reference fiche was to establish a complete health history as known to OHIP for every person included in the Plan, in every office that received a set of claims fiche.

Every physician and hospital in the province has been assigned a number. There exist diagnostic codes and fee schedule codes. With possession of the code books, which are readily available at every OHIP office, one is able, from the claims fiche, to determine information under the following categories for every service performed:

1. clinic number, if there is a clinic number;
2. practitioner's number;
3. the practitioner's speciality code;
4. physician's accounting;
5. whether it was a referral;
6. the number of the clerk who did the assessment;
7. the date on which the assessment was done;
8. the claim number for each service;
9. the item number;
10. the hospital admission date if there was a hospital admission;
11. the diagnostic code;

12. the fee schedule code;
13. the date on which the service was performed;
14. the number of services performed; and
15. the fees billed, approved and paid.

Normally, every family has one number with the result that all services rendered to a given family are grouped together on the claims fiche. OHIP also produces: (1) an alpha-fiche which is an alphabetic listing of all pay-direct subscribers and group subscribers showing, for the pay-direct subscribers, their home addresses, and for the group subscribers, the names and addresses of their employers, and (2) enrolment fiche, a numeric listing of all subscribers in which the enrolment data is keyed to OHIP number.

Information about a physician's treatment of a patient enters the OHIP system by the processing of a physician's claim card. For the purposes of my discussion of the involvement of police with OHIP, I need not elaborate on this aspect of the process. However, a short description is necessary of the means by which information from hospitals, concerning hospital attendances, enters the OHIP system. Information about a patient's hospital admission and the diagnosis made during a hospital stay comes into the OHIP system as a result of a complex process. The patient attends at the hospital. If admitted, an admission form, Form 106A, is prepared by the hospital staff and sent to OHIP. On its receipt, a data entry process checks eligibility and, if the patient has coverage, a discharge form, known as Form 106D, is sent by OHIP to the hospital. If the patient was not a subscriber or a dependant of a subscriber and did not meet OHIP's eligibility requirements, a non-OHIP discharge form is sent by OHIP to the hospital.

When the patient is discharged, Form 106D is completed at the hospital. This document contains the patient's name, address, OHIP number, and a diagnostic code which depends upon the diagnosis made and the procedure performed. Form 106D is returned to OHIP where it is checked, processed, coded, if necessary, and the information contained on the form is entered, during a data entry process, into the claims reference file. On completion of the data entry process, the completed Forms 106D are stored, by hospital, at the Toronto District OHIP office, 2195 Yonge Street. Approximately 1.2 million of these forms are processed and stored yearly.

The Health Insurance Act, 1972, as amended by S.O. 1974, chapter 60, section 9 and chapter 86, section 2, imposes a general obligation of confidentiality on all OHIP employees. The



Monthly, sets of claims fiche are shipped, as indicated below, to the various OHIP district offices throughout the Province:

<u>Number of sets shipped</u>	<u>Location of District Office</u>
2	Mississauga
2	Oshawa
1	Ottawa
4	Hamilton
2	London
1	Kingston
1	2195 Yonge Street, Toronto
1	Sudbury
1	Thunder Bay

Many district offices control satellite offices. These district offices sometimes ship the previous month's claims fiche to satellite offices. Prior to the commencement of our hearings, there were no effective controls on distribution or destruction or a consistently implemented destruction policy for these microfiche. The claims fiche contain, in easily readable form, all health information maintained by OHIP about all subscribers and their dependants. The effect of this distribution of the claims reference fiche was to establish a complete health history as known to OHIP for every person included in the Plan, in every office that received a set of claims fiche.

Every physician and hospital in the province has been assigned a number. There exist diagnostic codes and fee schedule codes. With possession of the code books, which are readily available at every OHIP office, one is able, from the claims fiche, to determine information under the following categories for every service performed:

1. clinic number, if there is a clinic number;
2. practitioner's number;
3. the practitioner's speciality code;
4. physician's accounting;
5. whether it was a referral;
6. the number of the clerk who did the assessment;
7. the date on which the assessment was done;
8. the claim number for each service;
9. the item number;
10. the hospital admission date if there was a hospital admission;
11. the diagnostic code;

12. the fee schedule code;
13. the date on which the service was performed;
14. the number of services performed; and
15. the fees billed, approved and paid.

Normally, every family has one number with the result that all services rendered to a given family are grouped together on the claims fiche. OHIP also produces: (1) an alpha-fiche which is an alphabetic listing of all pay-direct subscribers and group subscribers showing, for the pay-direct subscribers, their home addresses, and for the group subscribers, the names and addresses of their employers, and (2) enrolment fiche, a numeric listing of all subscribers in which the enrolment data is keyed to OHIP number.

Information about a physician's treatment of a patient enters the OHIP system by the processing of a physician's claim card. For the purposes of my discussion of the involvement of police with OHIP, I need not elaborate on this aspect of the process. However, a short description is necessary of the means by which information from hospitals, concerning hospital attendances, enters the OHIP system. Information about a patient's hospital admission and the diagnosis made during a hospital stay comes into the OHIP system as a result of a complex process. The patient attends at the hospital. If admitted, an admission form, Form 106A, is prepared by the hospital staff and sent to OHIP. On its receipt, a data entry process checks eligibility and, if the patient has coverage, a discharge form, known as Form 106D, is sent by OHIP to the hospital. If the patient was not a subscriber or a dependant of a subscriber and did not meet OHIP's eligibility requirements, a non-OHIP discharge form is sent by OHIP to the hospital.

When the patient is discharged, Form 106D is completed at the hospital. This document contains the patient's name, address, OHIP number, and a diagnostic code which depends upon the diagnosis made and the procedure performed. Form 106D is returned to OHIP where it is checked, processed, coded, if necessary, and the information contained on the form is entered, during a data entry process, into the claims reference file. On completion of the data entry process, the completed Forms 106D are stored, by hospital, at the Toronto District OHIP office, 2195 Yonge Street. Approximately 1.2 million of these forms are processed and stored yearly.

The Health Insurance Act, 1972, as amended by S.O. 1974, chapter 60, section 9 and chapter 86, section 2, imposes a general obligation of confidentiality on all OHIP employees. The

exact statutory provision is of such importance that I set it out in full:

44.(1) Each member of the Medical Review Committee, every practitioner review committee, the Medical Eligibility Committee and the Appeal Board and each employee thereof, the General Manager and each person engaged in the administration of this Act and the regulations shall preserve secrecy with respect to all matters that come to his knowledge in the course of his employment or duties pertaining to insured persons and any insured services rendered and the payments made therefor, and shall not communicate any such matters to any other person except as otherwise provided in this Act.

(2) A person referred to in subsection 1 may furnish information pertaining to the date or dates on which insured services were provided and for whom, the name and address of the hospital and health facility or person who provided the services, the amounts paid or payable by the Plan for such services and the hospital, health facility or person to whom the money was paid or is payable, but such information shall be furnished only,

- (a) in connection with the administration of this Act, The Medical Act, The Public Hospitals Act, The Private Hospitals Act, The Ambulance Act, or the Hospital Insurance and Diagnostic Services Act (Canada), the Medical Care Act (Canada), or the Criminal Code (Canada), or regulations made thereunder;
- (b) in proceedings under this Act or the regulations;
- (c) to the person who provided the service, his solicitor or personal representative, the executor, administrator or committee of his estate, his trustee in bankruptcy or other legal representative;

(d) to the person who received the services, his solicitor, personal representative or guardian, the committee or guardian of his estate or other legal representative of that person; or

(e) pursuant to a subpoena by a court of competent jurisdiction.

(3) The information referred to in subsection 1 may be published by the Ministry of Health in statistical form if the individual names and identities of persons who received insured services are not thereby revealed.

(4) The General Manager may communicate information of the kind referred to in subsection 2 and any other information pertaining to the nature of the insured services provided and any diagnosis given by the person who provided the services to the statutory body governing the profession or to a professional association of which he is a member.

OHIP employees must preserve secrecy with respect to all matters related to the administration of the Act. The exceptions to the general obligation of confidentiality permit disclosure of certain specified information. These exceptions do not permit disclosure to the police of either diagnostic or fee-schedule information under any circumstances whatsoever. Despite this clear and unequivocal prohibition, OHIP's policy was one of co-operation with police forces. The only written directive, at OHIP, dealing with confidentiality was set out in an enrolment manual of limited circulation which stated that:

A subscriber's OHIP records are to be treated as confidential and are not to be available to general inquiries. In situations involving police matters, the inquirer's identity, rank and location must be established and confirmed before any information can be given concerning an OHIP subscriber.

Gordon Ellis Fetherston, the General Manager of OHIP until 1979, became an employee of the Ontario Hospital Services

Commission in 1958. In 1971, he chaired a committee which looked into the mechanics of amalgamating the Ontario Hospital Services Commission and the Health Services Commission. On amalgamation, in 1972, he was appointed General Manager and acquired the general responsibility for the operation of the OHIP system. Mr. Fetherston testified that it was Ontario Hospital Services Commission policy, on request, to give enrolment information, addresses, names, and OHIP numbers to the immigration department and to the police. When OHIP was established on April 1, 1972, the same policy was continued, despite the language of section 44 of The Health Insurance Act, 1972. Mr. Fetherston knew that this was the policy. When asked how he could reconcile this policy with section 44 he replied that he "didn't even think about it." Neither Mr. Fetherston nor any other OHIP employee requested a legal opinion as to whether or not the practice being followed could be reconciled with section 44. Mr. Fetherston's own testimony was that he had probably not directed his mind to section 44 of the Act and the policy of disclosing information to the police prior to 1977.

Many OHIP employees gave evidence at our hearings. It is clear that the prevailing belief prior to November, 1977, was that co-operation with the police when information was requested was expected and required. Some employees believed that any kind of information could be disclosed. This was understandable. There was no detailed directive outlining what information might be disclosed and under what circumstances disclosure could occur. It is against this prevailing policy and attitude that police conduct must be examined.

The Royal Canadian Mounted Police is, of course, a federal police force. Outside of Ontario, it is structured, for command purposes, by provinces. Ontario, because of its geographic size, has been divided into three different divisions: (1) O Division--centred in Toronto and responsible for southwestern Ontario, (2) A Division--centred in Ottawa and responsible for the north-east part of the Province, and (3) D Division--which is responsible for the extreme north-west part of the Province and which is centred in Winnipeg. Internally, the force is divided into two branches, criminal investigation and the security service. Ontario is organized as described above for both branches.

Criminal investigation and security services have distinct and separate responsibilities. Criminal investigation is responsible, for example, for enforcement of the criminal law, and the law relating to narcotics and customs and excise. The security service is responsible for domestic security and also for



field investigations for security clearances for federal government employees when requested by various federal departments.

Prior to November, 1977, the RCMP routinely obtained information from OHIP in circumstances which amounted to violations of section 44 of The Health Insurance Act, 1972.

Before describing the contacts between members of the RCMP and OHIP, it would be helpful to define some of the terms encountered in the evidence. Chief Superintendent Michael Spooner, then the Area Commander for the Southwest Ontario Security Service, and a member of the Security Service of the RCMP for 21 years, testified at our hearings in November, 1978. I was given an explanation of who, in common security terminology, was a "legal intelligence officer". Chief Superintendent Spooner said that a legal intelligence officer was a representative of an embassy's accredited staff. This person had a legitimate function to perform such as, for example, that of a chauffeur or trade counsellor. Usually, the RCMP was aware that this person's principal function was that of an intelligence officer whatever role he or she might be playing.

"Illegal intelligence officers or agents" are persons who are in Canada under an assumed identity. The identity is usually that of a Canadian, who, at one time, was repatriated to a country behind the iron curtain and who had died and had his or her place taken by this "illegal". Sometimes the identity taken is that of a person who died in Canada. The illegal may have identification from another country, for example, Mexico or Germany, and use this fake documentation to make an apparently proper entry into Canada. These persons are also known as "deep cover agents". Residing in Canada, for all intents and purposes they function as legitimate Canadian residents. They are able, either regularly or irregularly, to assemble intelligence information for their hostile intelligence service. This type of agent may even function as a "sleeper", that is, as an ostensibly legitimate member of Canada's society, for many years until required to provide or perform a particular service for the organization. According to Chief Superintendent Spooner's evidence, the illegal agent is difficult to detect and, in the long run, is the type of individual capable of inflicting the greatest damage on Canada's national security.

The RCMP came into possession of information from a non-medical source that led it to believe that there was a deep cover agent functioning and residing in Canada. The RCMP did not know the agent's name and had no other information except certain particulars which, if revealed, would disclose matters of national security. For that reason I refrain from reciting

the true facts and explain the nature of the matter by a hypothetical account. The RCMP learned that the deep cover agent was a male, aged 50, who, during August, 1977, in the Niagara district had been treated in a public hospital for a sprained ankle. Inspector Randall Claxton was provided with this information and instructed to locate the deep cover agent. Inspector Claxton reported to Chief Superintendent Spooner who, in turn, reported to the Deputy Director General of Operations of the Security Services in Ottawa. The file containing this information was marked and continues to be marked "Top Secret".

It was Inspector Claxton's responsibility to co-ordinate the investigation aimed at identifying this deep cover agent. He authorized members of the RCMP to attend at OHIP in an attempt to obtain the names of individuals possessing those characteristics, that is, males who were aged 50 and who were treated in August, 1977, in the Niagara district for a sprained ankle. The decision to seek out information from OHIP was made by Inspector Claxton and he was the most senior RCMP officer aware that members of the force intended to attend at OHIP for this investigation. The RCMP, as a force, has accepted responsibility for Inspector Claxton's decision.

Inspector Claxton also testified at our hearings. He described this information as sensitive and "perishable" because, unless the RCMP reacted quickly, the information would become useless. He made preliminary inquiries and concluded that it would be "beyond burden" to approach every hospital in the geographical area involved. He therefore gave instructions to Corporal Peter MacNeil to attend at OHIP to inform senior OHIP officials of the nature of the problem and to ask for permission to review hospital discharge records at their final repository, which was the Toronto District office of OHIP at 2195 Yonge Street. Inspector Claxton said that, as a "line officer", it was within his prerogative to make this decision. He testified, and I accept his evidence, that he was unaware that OHIP employees were under an obligation to keep information confidential and that this was the first and only time that he had ever directed, or arranged for any person to attend at OHIP to seek information. He had deduced that OHIP was the only logical source from which this information could be linked to a named individual or individuals.

In accordance with his instructions, Corporal Peter MacNeil went to the OHIP office. He spoke to a senior person there, identified himself and, in general terms outlined the identifying factors with which he was working. Evidence was given in camera by that senior OHIP person. It would not be in the public interest to identify this individual. Corporal MacNeil

clearly and fairly identified himself and his purpose and informed the official that the RCMP were seeking an agent of a foreign power and that this matter involved national security. The senior OHIP official authorized Corporal MacNeil and Corporal John McQueen Appleton to attend at 2195 Yonge Street to review the 106D hospital discharge forms. Corporals MacNeil and Appleton then reviewed more than 100,000 claims cards. They photocopied 82 of them and forwarded the photocopies to Ottawa where they remain in RCMP possession. Both men testified that they had attended at the OHIP office because of their direct order from Inspector Claxton and that their attendance was for this purpose only.

I reviewed the Top Secret RCMP file in camera. My conclusion, from all the evidence, is that, at the time of their members' attendance at OHIP, the RCMP was involved in a genuine intelligence operation, the purpose of which was to locate a deep cover agent of a foreign power. It is clear, however, that section 44 of The Health Insurance Act, 1972 does not sanction this course of action. Health information was, in fact, disclosed to the RCMP which could not be released under any circumstances whatsoever under the current state of the law and under the law as it then existed.

It may not be out of place to express the view that it was surprising that the RCMP and the senior OHIP official would resort to a manual review of such a large number of cards for the purpose for which it was undertaken. As pointed out earlier, all information that OHIP has finds its way into the claims reference file. It would have been a simple matter to write a computer program to extract all entries on the claims reference file which answered the description of all the variable factors known to the RCMP. This approach, had it been taken, would have provided a complete listing of all of the persons of that description without exposing to the RCMP the personal information of thousands of others. There was no satisfactory explanation of why such a procedure was not followed. I make this point, not to give approval to this method, but only to illustrate other means of access to the information should it be concluded that the law should be amended to sanction access of this kind.

There were other RCMP contacts with OHIP. Some of them took place during RCMP monitoring of alleged "violence-prone individuals and groups". Chief Superintendent Spooner testified that the RCMP Security Service, on the direction of the federal Cabinet, had the responsibility of monitoring and investigating persons and groups of this description. His evidence in this respect was as follows:

Q. In the fall of 1974, did the RCMP have responsibility to monitor certain organizations?

A. That's correct, sir.

Q. What types of organizations would the RCMP be...

A. Under the mandate given to the RCMP Security Service by the government, included in that mandate are the monitoring and investigation of violence-prone individuals and groups.

Q. Is that a directive that the RCMP gets from the federal government?

A. These are, perhaps I can describe it as guidelines provided initially by the Cabinet. Those guidelines are interpreted by senior committees of the government in Ottawa as part of the national security and intelligence apparatus within the national capital and these committees in turn provide specific direction to the RCMP Security Service in terms of interpreting the government's mandate as it applies to organizations.

Q. That is important because it is not a followup of the RCMP on its own?

A. Not at all, sir.

Q. This is really the monitoring, if I understand your evidence, of these violence-prone organizations or groups who are perceived to be violence-prone?

A. That is correct, sir.

Q. It is undertaken as a direct response to a directive from the federal government?

A. That's correct sir.

For the purpose of discharging this obligation, Corporal Gene Raymond Young Montgomery, in the fall of 1974, attended at



OHIP's District Office in Thunder Bay. He identified himself as a member of the RCMP and spoke to Allan Chaplin who was then the Thunder Bay District Claims Manager. Mr. Chaplin referred Corporal Montgomery to Herman J. Arkelian, then District Director of that office. Corporal Montgomery had asked Mr. Chaplin to supply him with addresses for certain individuals because, as Mr. Chaplin related the conversation, "these people that he wished to locate could possibly have something to do with going against national security." Corporal Montgomery "implied" that the political beliefs of these individuals could be detrimental to the nation. Corporal Montgomery admitted that he had made mention of a "left wing or Communist group or organization". Mr. Arkelian agreed to provide this information. Corporal Montgomery sought the addresses of two individuals who stood for election to Parliament in 1974 on behalf of the Communist Party of Canada, Marxist Leninist Group. As it transpired, OHIP was not able to provide their addresses. Although no medical information was sought or received, it seems to me, nevertheless, disquieting that the RCMP utilized OHIP in an attempt to carry out surveillance of two persons who had run for Parliament in 1974 on behalf of a lawful political party. Despite Chief Superintendent Spooner's evidence that these inquiries had nothing to do with the political campaigns which, at the time of the inquiries, had recently taken place, I do not know the reason for this investigation.

Chief Superintendent Spooner went on to testify that the characterization of a particular organization as violence-prone and one therefore to be monitored, were not judgments made by an individual RCMP member. He referred to the Operational Priority Review Committee. His evidence in this respect was as follows:

There is a senior committee which sits in Ottawa. It is a committee, it is called the Operational Priorities Review Committee. It is made up of senior members of the Security Service from the rank of Superintendent and Chief Superintendent.

. . . . .

[The Operational Priorities Review Committee] also has a member of the, a lawyer from the Department of Justice is also a member of this committee, as is a senior officer of the Criminal Investigation Branch. The purposes of this committee is to interpret the mandate given to the Security Service by the government in terms of directing us to



investigate certain organizations or individuals. It also serves as a committee to which, if new organizations are identified, for example, in an area, the information regarding them is forwarded to headquarters for a decision from them as to whether this is a group which falls within the mandate of the Security Service and whether investigation of this group is authorized. So a young member has no, cannot exercise his own initiative in this regard. He can only exercise initiative in the ways in which he investigates it, but what he investigates, the groups he investigates, is determined by this senior policy group at headquarters and on a day to day basis by senior commanders such as myself or other senior officers working for me.

There is confusion in this testimony. Chief Superintendent Spooner's explanation was made with respect to questions relating to the investigation of two candidates for office that took place in 1974. The explanation given, however, describes a state of affairs that did not then exist. Although the answer cannot be characterized as inaccurate because the question was phrased in the present tense, I confess that I interpreted it as relating to 1974. In fact, however, testimony given before the McDonald Commission, the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, makes it clear that the Operational Priorities Review Committee was conceived of by senior officials of the Security Service in February, 1977, and came into existence only after that date.

As I have indicated, the explanation of the reason for which information was being sought from OHIP about the two former candidates remains a mystery. My terms of reference, in the light of the prevailing constitutional limitations, make it impossible for me to compel the RCMP to disclose the reason for the inquiry. This illustrates the serious difficulty in making recommendations with respect to access to a provincial source of information on the part of a federal force that cannot or will not be made answerable to provincial authorities in the event of, or to ensure the prevention of, abuse of the right of access. The RCMP points to national security as justification for having sought confidential information, including health information, from a provincial authority. This action involved the provincial authority in a violation of provincial legislation which, given the current state of that legislation, cannot be justified. But I have been asked to recommend changes in the

legislation which would sanction the practice of receipt by the RCMP of information from OHIP in, among other cases, national security situations. As I have said, however, the RCMP is not subject to provincial scrutiny or accountability which would ensure that the information sought was for purposes, and was being sought in circumstances, which the Province of Ontario considered proper. History does not justify blind trust or confidence that confidential health information would be obtained only in situations authorized by the current state of law as it may exist from time to time. The circumstances of this episode of RCMP access to OHIP information is all the more disturbing because it was revealed by our own investigation and not disclosed to us by the RCMP.

I move now to the subject of security clearances. Our investigation revealed that the RCMP contacted OHIP and obtained confidential health information from this source on two occasions in the discharge of their responsibility for security clearances. Under the federal Cabinet's Directive No. 35, the RCMP is authorized and required to conduct security screening of federal employees or prospective government employees who are to be given access to classified information. There are three categories of clearance, namely, confidential, secret and top secret. The procedure followed by the RCMP varies with the category of clearance desired.

Most federal departments have a departmental security officer whose responsibility is to ensure that employees are properly cleared to carry out the functions within their job specifications. If a "confidential" clearance is required, all that is necessary is that the subject's finger prints be submitted to permit the criminal indices to be searched and a check is made of his or her name and address in the "subversive indices" maintained by the RCMP. The results of these checks are returned to the departmental security officer. If a clearance at the "secret" level is required, the same procedure is followed as in the case of a confidential clearance but, in addition, the department security officer has the option of requesting the RCMP to carry out a field investigation. If a "top secret" clearance is sought, the same procedures are followed as at the confidential level but, in addition, the RCMP is required to carry out a full field investigation. As explained by Chief Superintendent Spooner, this requires the RCMP to examine and report on "the person's background, character, employment over the previous 10 years of their life or back to the age of 18, whichever comes first in the case of the young person...[and] conduct these field investigations" and to determine whether the applicant is a person in whose reliability and loyalty to the country the Government of Canada can repose full confidence.

These requirements are contained, as I have stated, in Cabinet Directive No. 35, which is of such interest and gives such a complete description of the procedure involved and the information sought with respect to security clearances that it is reproduced in full as an appendix to this section. The accompanying Memorandum for Deputy Ministers and Heads of Agency dated December 27, 1963, appears as Appendix II. The procedure was varied in May of 1975 to conform with amendments to the Financial Administration Act in 1967 (S.C. 1966-67, chapter 74) with respect to the treatment, including discharge, of employees on security grounds. A memorandum dealing with this Amendment to Cabinet Directive No. 35 appears as Appendix III to this section.

For a top secret clearance, part of the examination of the subject's background involves a review of the personal history form completed by him or her. This form is very detailed in nature and contains, as might be expected, a great deal of highly personal information, including information about the subject's relatives, both by blood and by marriage. Perhaps the most significant feature of the personal history form, however, is the complete absence of anything on the form in the nature of a consent or permission by the subject to the obtaining of any health information about him or her.

The RCMP member carrying out the field investigation normally reviews all references on the form, checks with neighbours for general information from them and other persons who might reasonably expect to have some knowledge of the applicant for security clearance and, eventually, completes a report. The field report is returned to RCMP headquarters in Ottawa and to the branch responsible for overseeing security and which contains a small group of analysts and brief writers. A brief is made from the field report. The brief is really a summary of the facts disclosed by the investigation. The contents of the brief are classified as either confidential or secret and the brief is forwarded to the responsible departmental security officer. The departmental security officer is not entitled to receive the original field report or reports and is never given access to these reports. The brief sent to the departmental security officer contains the following statement:

This document is the property of the RCMP security service and is loaned to you for the confidential use of the Minister, the Deputy Minister as well as the designated security officer. This document, its contents or any part thereof is not to be

copied or further disseminated without the prior consent of the originator.

Special Constable Peter Roger King is employed by the RCMP Security Service. A special constable is a formal rank which is given to members of the RCMP who are engaged, more or less, in one particular job or function. Special Constable King was primarily concerned with security clearance investigations in Toronto. In late 1975, the Department of Public Works requested a security clearance for an employee who, at our hearings, was called Mr. X to avoid any invasion of his privacy, a procedure we followed throughout the inquiry whenever an individual's health information was to be disclosed. During the course of his investigation, Special Constable King attended at the offices of OHIP in Toronto after he had reviewed X's file. The file disclosed that Mr. X had had psychiatric problems, had been hospitalized in 1958 for these problems, and had been diagnosed as a manic depressive and alcoholic with various other problems. Special Constable King explained his thought process in the following exchange:

Q. All right. Did you in the course of the inquiries being made go to the OHIP office?

A. I did. Yes, sir.

Q. Why?

A. I had checked the file before I commenced the inquiry and the file indicated that Mister X had had psychiatric problems and had received hospital treatment in 1958 for psychiatric problems. This indicated an area which I should go into as deeply as I could.

Q. Why?

A. Because in addition to the loyalty and discretion of my subject, I have to be concerned with his reliability. Any mental instability would be a factor concerning his reliability so I considered that this was something I had to go into as deeply as possible.

Q. What did you do?

A. I went to OHIP...

Q. I'm sorry. Just before we get into that, did you know what the earlier diagnosis was?

A. I believe it involved manic depressive alcoholism, various other problems. But it generally indicated to me that there were psychiatric problems that, which would indicate mental instability.

Q. So you read the file, you found out about this information?

A. Yes.

Q. You found out it was obtained from a psychiatric facility in the province and you made a decision to go where?

A. To the OHIP head office on Overlea Boulevard.

Q. Why did you decide to do that?

A. I wanted to see if he was currently or had been receiving any kind of treatment for a psychiatric condition since the previous inquiry.

Q. Had you gone there any previous time?

A. I may have gone once before. I can't remember if it was before or afterwards, but that was nothing to do with medical information. I did go to interview somebody with connection with, an applicant for employment. I believe the person I went to see was a character reference, sir. It had nothing to do with medical information at all.

Q. Had you ever gone seeking any medical information or enrollment information?

A. I have never been to OHIP in that respect.

Q. What made you decide to go that time? The time relating to Mr. X?



A. Because I thought it possible that I might find information which would indicate if he had been receiving hospital or medical treatment for a psychiatric condition.

Q. Did anyone else who was involved in security clearances suggest to you that you go to OHIP?

A. No. It was my decision.

Q. It was your own decision? No help or hint from any person or any book or any digest or anything else?

A. Well, no, I was assigned to the investigation and it was my decision to go there.

When Special Constable King attended at the OHIP offices, he identified himself to an unknown official and explained that he was seeking information about Mr. X. He was told that the record of X was not in Toronto and that he would have to go to another district office. This statement makes no sense because the health records of all persons with OHIP coverage are in every District Office throughout the Province. It is a reasonable inference that the unknown OHIP official whom Special Constable King approached did not want to assist him but, on the other hand, did not want to appear unco-operative. He suggested that Constable King contact a Mr. Albert Board who was described by this official as "well motivated towards security". After obtaining this information, Special Constable King wrote a report suggesting that an inquiry be made at the Hamilton District Office. As a result, in January, 1976, a directive went from Special Constable King to Corporal Glen Allan Gartshore of the RCMP outlining the need for a security clearance for Mr. X and the need to confirm medical treatment for a medical disorder. Mr. X's OHIP number was given and Mr. Board was named as the person to be contacted at the Hamilton District Office of OHIP. Corporal Gartshore testified, and I accept his testimony, that he had never contacted Mr. Board prior to January, 1976, when he attended at the Hamilton District Office. Corporal Gartshore identified himself to Mr. Board and explained that he was conducting a security clearance investigation and required information confirming medical treatment for Mr. X. Mr. Board, in turn, explained that it would be necessary to translate from code the physicians' numbers and diagnostic codes. Corporal Gartshore provided Mr. Board with Mr. X's OHIP number which he had received from Special Constable King. In his testimony, Mr. Board acknowledged that Corporal Gartshore had attended upon

him. He agreed that Corporal Gartshore properly identified himself and, as he put it:

...I was advised that the people were either employed or were about to be employed in a highly sensitive area of the Federal Government operation which was related to National Security. That the people involved were aware that security checks were being made on them and had agreed to them.

Mr. Board stated his understanding of OHIP's policy, insofar as it related to co-operation with police, to be as follows:

It was my understanding that we would co-operate fully with any law enforcement agency in the execution of their legitimate duties.

Mr. Board asked his secretary to obtain a printout relating to Mr. X from the claims reference microfiche. He provided Corporal Gartshore with the dates upon which Mr. X had received medical treatment since 1972, the names of the general practitioner and psychiatrist who had treated Mr. X, the dates of birth of Mr. X's wife and children, the OHIP diagnostic code numbers relating to every visit to the physicians and a translation of these code numbers. He also informed Corporal Gartshore that members of Mr. X's family had also undergone psychiatric treatment. As a condition of payment by OHIP, physicians are required either to use a description on the claim cards which they submit or to insert a diagnostic code. If a description rather than a code is used, the description is translated by an OHIP clerk to the appropriate diagnostic code. The codes are broad in scope. Mr. Board explained to Corporal Gartshore that the codes covered a wide range of diagnoses.

The diagnostic codes 300 and 303 described Mr. X's visits to his psychiatrist. The codes translate as:

CODE 300

Anxiety (reaction, state, neurosis)  
Cancer Phobia  
Claustrophobia  
Emotional Instability  
Hysteria  
Impulsive Neurosis  
Manic Depression (Acute)  
Nervous Breakdown  
Nervous Collapse

Neurosthenia  
Neurosis (Unspecified)  
Obsessive Compulsive Insanity  
Psychogenic Cardiospasm  
Psychoneurotic Amnesia  
Psychoneurotic Disorders reaction  
    (Disassociative, Conversion, Phobic,  
    Obsessive, Compulsive, Depressive)  
Suicidal Tendencies

CODE 303

Alcohol Addiction (Chronic, Acute)  
Alcoholic Coma

What Corporal Gartshore did not learn was that OHIP's diagnostic code did not have a number for diagnosis of "normal" which would permit a psychiatrist to obtain payment. Nor was Corporal Gartshore aware that 300 was a very common diagnostic code because this number includes an "anxiety state", however minimal that state may be. In any event Corporal Gartshore dutifully included this information in his report and, as a result, Mr. X was denied security clearance.

Nor was this the only occasion that Corporal Gartshore contacted Mr. Board. In July, 1977, Corporal Gartshore was ordered to undertake a security screening investigation by Sergeant Farrell of the RCMP in Hamilton. This investigation involved a federal civil servant whose position required a top secret clearance. Corporal Gartshore once again attended at Mr. Board's office and eventually gave Mr. Y's OHIP number to Mr. Board. Again he told Mr. Board that the matter was one of national security. After obtaining the information from the claims reference microfiche, Mr. Board gave Corporal Gartshore the name of Mr. Y's spouse, the name of Mr. Y's treating physician and that of his spouse, the dates of treatment and the diagnostic code numbers. Corporal Gartshore knew that Mr. Y had possibly previously seen a psychiatrist. As indicated, Mr. Board again provided Corporal Gartshore with the codes, which were 300, 780 and 799. Code 780 translates as "signs and symptoms not yet diagnosed, convulsions, ataxia, vertigo, amnesia and tenitis". Code 799 is "not yet diagnosed". Corporal Gartshore testified that he had never attended at a physician's office as a result of the information given to him by Mr. Board. As a matter of interest, despite this information, Mr. Y was granted the security clearance sought.

Mr. Board's disclosure of the information to Corporal Gartshore was in violation of The Health Insurance Act, 1972. However, his conduct is understandable in the light of the

philosophy by which OHIP governed itself in the period April, 1972, to November, 1977. Its policy was one of full co-operation with the law enforcement agencies. On every occasion on which he was contacted by the RCMP or other police departments, Mr. Board required an explanation of the purpose for which the police were seeking information. He was, in effect, relying on the integrity of the police officer who was making the representation to him to ensure that the matters under investigation were legitimate police matters. When Corporal Gartshore spoke to him of "national security", Mr. Board naturally thought of issues of significant state importance. Having heard evidence of the precise positions of Mr. X and Mr. Y, I can express my opinion that their jobs cannot reasonably be characterized as matters of state importance and national security.

Mr. Board's disclosure of the information he gave Corporal Gartshore and, in fact, his co-operation generally with the police, were no more than the logical outgrowth of the long standing OHIP policy. Notwithstanding section 44 of the Act, this policy had the approval of senior officials to the General Manager level of OHIP. Although Mr. Board ought to have complied with section 44, it is understandable that he did not.

Mr. Board estimated that he had been contacted by the RCMP on an average of a "couple of times per year". He had no record of the visits and his estimate was guesswork. The RCMP did not have, or was not able to locate records of such frequent visits. Mr. Board's position with respect to this estimate may be seen in the following extract of the cross examination by Arthur Pennington, counsel for the RCMP and the Solicitor General of Canada:

A. I was initially asked if I had given medical information to RCMP officers. My answer was it is very probable. That is as far as I could really go. It was probable. When it was pointed out to me that the officers were obtaining this information for security checks, then another little piece of the jigsaw puzzle fell into place and I said yes, that the RCMP officers had been in the Hamilton district office for the purpose of security checks and it is very probable that I gave the information that they say I gave. But I have no definite recollection of what information was given. I have no definite recollection as to how many times I was asked. I was asked, well was it twice a

year? And it could have been twice a year. As I mentioned, it is not a part of my job which relates to my achievement of my objectives. It is a situation where we tried to be co-operative with the police in the execution of their duties. It didn't relate directly to the execution of my duties. So it was a matter of determining the credentials of the individual, co-operating to the best of my ability, and that was, as far as I was concerned, the end of the incident.

When I say that it could have been twice a year since 1972, it might have been one year or nothing in one year, two or three times...

Q. Is it...

A. ...and I also want to make it clear that I am not saying that medical information was given out at every incident. It's a matter of how many times have the RCMP been in your office and to the best of my belief I would say it would average maybe twice a year at the most.

Q. At the most?

A. At the most.

Q. I would like, if I can, to pursue it a little farther and correct me if I am wrong because I don't want to push you to be saying things that you really don't feel, but my impression is that what you are telling us now is a general impression that you have in retrospect looking back. It is an impression you have?

A. Correct.

Q. Is it also not correct to say that you cannot say positively that medical information was given on any occasion other than the two instances relating to Corporal Gartshore?

A. Correct.



Q. That the frequency that you have told us about, and I think you have made it clear just how indefinite that is, the frequency is at best an approximation and a maximum approximation?

A. Correct.

Q. It could have been much less than that?

A. That's right.

MR. COMMISSIONER: Well, you say that's right. It couldn't be much less unless it was zero? When you've got a figure of two, much less seems to me to be, to mean zero.

A. It could be zero. If you said how many times did the RCMP visit the office in 1973...

MR. COMMISSIONER: Oh, in a given year?

A. Yes.

MR. COMMISSIONER: But you made it clear that you were talking of an average. It may be, I thought you said, a year in which there was no contact and there may have been another year in which there were three?

A. That's right.

MR. COMMISSIONER: So it couldn't be much less than an average of two a year unless it was, as I say, a nil figure.

MR. PENNINGTON: Q. Have you had occasion to have inquiries made in your office as to this subject of the police contacted with the office?

A. Yes. I have made it very clear that if there is any contact by police officers that they should be referred to me.

Q. So that, I just want to be sure I follow. Was this an inquiry that you

instituted after this matter became a public issue?

A. No. That's been a general policy.

Evidence from employees of every OHIP District Office in Ontario was given at our hearings. It would be accurate to summarize the testimony by saying practically every employee who testified believed that co-operation with the police was the rule. Biographical data, that is, subscribers' names, home addresses, or employers' addresses, were routinely given to the RCMP, the Ontario Provincial Police and municipal police forces. There were many hundreds of contacts by various police forces throughout the Province with OHIP employees. Contact was so routine that no record was kept by OHIP employees with respect to the date of the contact, the name of the officer, the police force involved and the information provided. Nor did any police force keep a master record of these contacts. OHIP was a favourite and frequent source of information for police forces because it maintained the most up to date and comprehensive list of residents in the Province linked with current home address or employer's address.

There were hundreds of situations in which the RCMP contacted OHIP employees seeking biographical information. To give a clearer picture of the nature of police involvement with OHIP there follows an accurate summary introduced into evidence by the RCMP of the circumstances of some of their members' contacts with OHIP. Most of the contacts summarized have been confirmed by our independent investigation:

Corporal R.K. ABRAHAMSEN. A former Immigration and Passport investigator, Cpl. Abrahamsen made contact with OHIP by telephoning 482-1111 in Toronto but made no personal contact. He dealt with whoever would answer the phone and identified himself as an RCMP member and supplied sufficient information to OHIP personnel to confirm addresses and name of employer if it was available. He does not recall any particular case or OHIP employee. These inquiries all related to immigration investigations.

Corporal J. BEATON. Through investigative methods not involving OHIP the RCMP was aware that an espionage agent of a hostile foreign intelligence service was operating

in a specific geographical area in Canada sometimes after 1974.

. . . . .

Through other investigative methods, the RCMP compiled a list of, say, approximately 2000 suspected individuals in that geographical area, anyone of whom might be the "illegal" agent. A variety of investigative methods were used to narrow down this list of suspects. One of these methods was to contact OHIP and to use certain known pieces of information to rule out some of the names on the list. These pieces of information were not of a medical nature. An RCMP member contacted an OHIP employee identified himself as a member of the Force and requested assistance. The investigator furnished several names to the OHIP employee and asked the employee to search OHIP records for these names with a view to obtaining enrolment data (non-medical). A couple of weeks later the OHIP employee furnished enrolment data only to the member, as a result of which those names were eliminated from the list of suspects. Eventually all information pertaining to these names, including the enrolment data from OHIP, was destroyed and no record of it now remains in RCMP files. Cpl. Beaton had contacted the same OHIP employee sometime in 1973 concerning enrolment data with respect to the name of one person; Cpl. Beaton cannot now recall the name of the person or particulars of the case but he received no information with respect to the name.

Constable C.D. BARRETT. Presently a Toronto Immigration and Passport Investigator, Cst. Barrett contacted OHIP by telephone 965-8325 and talking to whoever answered. He identified himself as a member of the RCMP and supplied the OHIP number, name, date of birth of his subject and requested current residence address and name of employer. He did not request any other type of information and cannot recall the names of the persons he spoke to at OHIP or any

specific case. These inquiries all related to immigration investigations.

Constable T.J. BOYD. Cst. Boyd of the Toronto Immigration Section contacted OHIP at telephone number 482-1111 in Toronto and asked for a particular OHIP employee by name but cannot recall with any certainty this is the person he spoke to regarding the following inquiry. He states this is the person he would normally ask for upon calling OHIP. Cst. Boyd telephoned OHIP on May 5, July 21 and October 14, 1977 regarding a subject who was an illegal immigrant. He asked for the subject's residence address, name of employer, and the source of contributions. He was provided with an employer's name and address but the subject had left that company. A warrant for Arrest of the Subject remains outstanding.

Corporal J.G. CAMPBELL. A former Toronto Immigration and Passport Section Investigator/Supervisor, Cpl. Campbell made contact with OHIP by telephone and spoke to whoever answered. He identified himself as a member of the Force and requested information with respect to a person's address and employer. Cpl. Campbell cannot recall any particular case or the names of the personnel contacted. These inquiries all related to immigration cases. He does have a name of an OHIP employee in his personal telephone index. This name was provided to him by another member and entered in his telephone index a number of years ago. He does not recall specifically speaking to this person.

Constable J.P.P. CYR. A Toronto Immigration and Passport Section Investigator, Cst. Cyr contacted OHIP by telephoning 965-8325. Cst. Cyr does not recall the name of the person he spoke to at OHIP. He would identify himself as a member of the Force and request information on the current residence and employer of a subject he had under investigation. He did not receive any other type of information from OHIP and cannot recall any specific cases or names of OHIP

official contacted. These inquiries all related to immigration investigations.

Constable J.A. CRAWFORD. Presently a Hamilton Immigration and Passport Section Investigator, Cst. Crawford contacted OHIP at Hamilton twice that he can recall. He would call 528-3481 and after identifying himself as a member of the RCMP would talk to anyone answering the phone. He would identify himself, quote an OHIP number, if he had it, and request current residence addresses. He cannot recall any specific investigation or the name of the person contacted at OHIP. These inquiries all related to immigration investigations.

Corporal J.A.M. CLAYDON. Cpl. Claydon, presently a Section Investigator/Supervisor with Toronto Immigration and Passport Section, has made contact with OHIP by telephoning 482-1111 in Toronto. In these calls, Cpl. Claydon would identify himself as a member of the Force and would speak to anyone who answered the telephone. He would supply the OHIP number, date of birth or age and request additional enrolment information. Cpl. Claydon does not recall any specific cases or persons contacted.

Constable W.C. CRICH. Cst. Crich, while a member of the Ottawa General Investigation Section, contacted the Ottawa OHIP office by telephone on several occasions in September or October, 1977. He spoke with either one OHIP employee or another one. There are between three and five such inquiries in this series, all for the purpose of attempting to locate persons. All inquiries were for tracer information only on relatively minor files such as Income Tax inquiries, Excise Tax inquiries, etc. In all cases the results were negative as our investigator did not have the OHIP number of the person he was trying to locate. In view of the lack of success experienced by our investigator, he eliminated OHIP as a source of information and made no further contact.



Constable R.S. CAIRNS. When Cst. Cairns was stationed with the Toronto Drug Section of the RCMP in the Spring of 1975, he was involved in an investigation of a major narcotics importing case which resulted in the conviction of two persons in Canada (each sentenced to 7 years in prison) and one person in India. In the period between March 1 and June 10, 1975, a large number of packages containing narcotics were mailed to fictitious persons through postal box numbers in Ontario. During this period, Cst. Cairns telephoned unknown person or persons at 482-1111 in Toronto. He would furnish the person who answered the telephone the name of the addressee on the package and would request any information relating to residence address, date of birth, employer and employer's address. He did not request any other information. This involved an estimated twenty-five to thirty names. In some cases the OHIP person was able to confirm that the names were those of real persons on their enrolment records. In such cases, the OHIP person supplied Cst. Cairns with their additional enrolment information (of the kind described above). Subsequent investigation of these real persons through other channels established that none of them were, in fact, associated with illegal narcotic importation.

Sergeant L.W. DENDYS. A request for assistance was received by the RCMP from a friendly foreign intelligence agency which indicated that they believed that they had their country. The espionage agent was suspected of using credentials of Ontario origin to mask his true identity. The request from the friendly foreign intelligence agency was for the RCMP to ascertain if possible whether the Ontario credentials were in fact false. A great number of sources were investigated, only one of which was OHIP. Some time after 1972 Sgt. Dendys telephoned 482-1111, identified himself as a member of the RCMP and spoke with an unknown person who answered the telephone. This first OHIP employee referred him to a second

OHIP employee who, after being generally advised of the nature of the request, agreed to assist the RCMP investigation. This second employee indicated if there were no OHIP record in the name of the suspect that he would not telephone Sgt. Dendys back. The OHIP employee did not call back. From a variety of investigations the RCMP were able to confirm to the friendly foreign intelligence agency that the Ontario credentials of the suspected agent were false.

Constable D.L. FUDGE. A former Toronto Immigration and Passport Section Investigator, Cst. Fudge contacted OHIP by telephone and spoke to whoever answered his call. He identified himself as a member of the RCMP and gave the OHIP number he possessed and requested the contributor's name, address, and employer. Cst. Fudge recalls one particular investigation regarding a subject, an Immigration Act investigation concerning the failing to report change of status. In this case, the investigator learned of the OHIP number and, as a result of a check by telephone with OHIP, learned of the subject's employer's name. The subject was located at his place of employment and arrested. These inquiries all related to immigration investigations.

Constable G.L.S. PROUD. Cst. Proud, while stationed with the Toronto Immigration and Passport Section during the period from September, 1973 until November, 1977, contacted OHIP on various occasions, the date of which was unknown, at telephone numbers 965-8325, 965-0840 and 482-1111, extension 220 in Toronto. He does not recall the name of any OHIP employee he spoke to, nor does he recall any specific investigation. On these occasions, he was trying to determine the residence address, employer address and possible date of birth for a person whose name he already knew. No other information was requested. To the best of Cst. Proud's recollection, he did not ever receive the information he was seeking.

Constable K.L. GIBSON. Presently a Toronto Immigration and Passport Section Investigator, Cst. Gibson contacted OHIP by telephoning 482-1111 in Toronto and spoke to anyone answering the telephone. He identified himself as a member of the RCMP, supplied name, date of birth and OHIP number if he had it for the purpose of confirming the residence or employer of the person he was investigating. Cst. Gibson does not recall any particular case or the name of the person at OHIP contacted and never asked for any other but enrolment information. These inquiries all related to immigration investigations.

Constable W.L. GILKER. Presently a Toronto Immigration and Passport Section Investigator, Cst. Gilker contacted OHIP several times by telephoning 482-1111, extension 1537 in Toronto. He would identify himself as an RCMP member and supply the name, birth date and OHIP number if available of the subject and request confirmation of current residence and employer. Cst. Gilker never requested any other type of information and cannot recall any specific case or names of the persons at OHIP that were contacted. These inquiries all related to immigration cases.

Corporal W.P. HECKENDORN. Cpl. Heckendorn, when stationed with the Toronto General Investigations Section had contact with an OHIP employee at 2195 Yonge St., Toronto on September 23, 1975. This contact with OHIP was in relation to an investigation in connection with a missing person. Cpl. Heckendorn was attempting to determine a current address with respect to this person. Cpl. Heckendorn does not recall if he received this information and there is no record on file that indicated he, in fact, did. In this particular instance, Cpl. Heckendorn went personally to the OHIP office and asked the OHIP employee to check the OHIP records.

Constable B.J. JOHNSON. Presently a Toronto Immigration and Passport Section Investigator, Cst. Johnson contacted OHIP by telephoning 482-1111, extension 1537 in Toronto and spoke to anyone who answered. He identified himself as a member of the RCMP and sought information on current addresses and employers of subjects under investigation. No particular case or OHIP employee recalled. His inquiries all related to immigration investigations.

Constable W.S. JEFFERY and Constable P.G. HADLEY. Csts. Jeffery and Hadley were both members of Toronto Airport Drug Squad. Cst. Jeffery contacted one employee at OHIP, Box 1744, Station "R", Toronto on August 27, 1977, regarding a subject. Cst. Jeffery requested assistance in locating the subject's doctor to inquire about his health prior to his Court appearance. A second OHIP employee contacted Cst. Jeffery stating that he could not identify the subject without an OHIP number. Cst. Hadley contacted the second employee on February 2, 1977, and supplied an OHIP number. On February 23, 1977, a third OHIP employee replied to Cst. Hadley with the name and address of the subject's doctor and the fact that x-rays were taken on September 7, 1976, and the name of the Radiology Laboratory. The above contacts with OHIP were made by letter. The subject was charged May 19, 1976 with Importing under Section 5(1) of the Narcotic Control Act. Approximately 14 Kilos of hash oil had been found secreted in three scuba tanks in the subject's possession. The subject had purchased the tanks in Toronto just prior to leaving for South Africa. His defence was that he was engaged in scuba diving. It was learned from other non-medical sources that the subject had undergone major chest and lung surgery within two years of his arrest, which would tend to negate his physical ability to participate in scuba diving. It was intended that medical evidence would be subpoenaed; however, this was not necessary and the subject was convicted and sentenced to 7 years

imprisonment without the necessity of obtaining information from his doctor. Neither the subject's doctor nor the x-ray laboratory were contacted for information.

Constable G.M. JENKINS. Cst. Jenkins of the Toronto Commercial Crime Section personally attended at the OHIP office at 2195 Yonge Street, Toronto on July 22, 1977. He spoke to a female clerk, whose identity he did not obtain, seeking the residence address and type of plan for a subject whom he was investigating under the Income Tax Act. The OHIP employee provided the subject's address, that he was covered by self paid single plan and that he had paid a \$33.00 premium. The address supplied by OHIP served to confirm the address already known to our investigator.

Corporal B.W. MELANSON. Presently a Toronto Immigration and Passport Section Investigator/Supervisor, Cpl. Melanson made contact with OHIP by telephoning 482-1111, extension 1537 in Toronto and spoke to whoever answered the telephone. He identified himself as a member of the RCMP and supplied the name and birth date of a person under investigation. Cpl. Melanson requested current resident address or employer's address. He never requested any other type of information and cannot recall any specific investigation or person who he called at OHIP. These inquiries all related to immigration investigations.

Constable S.L. MOORE. Presently a London Detachment Immigration and Passport Section Investigator, Cst. Moore contacted the OHIP office at London by calling 437-4561 and spoke to an OHIP employee. He identified himself as a member of the Force and requested a current address for a subject, who was being investigated under the Canadian Immigration Act. The address obtained from OHIP was the one already known to the investigator and the subject of the investigation was never located. Whenever OHIP cards were recovered from illegal immigrants who were



deported, Cst. Moore would return them to the OHIP Claims Manager in Toronto.

Constable P.W. MacLEOD. A former Toronto Immigration and Passport Section member, Cst. MacLeod called OHIP to confirm OHIP card authenticity and possible addresses for subject. He also contacted OHIP concerning the returning of OHIP cards found in Immigration investigations. Cst. MacLeod made contact by telephoning 482-1111, local 1537 in Toronto and at a later date by phoning 965-8363. He also confirmed by letter when returning OHIP cards. Cst. MacLeod recalls contacting a particular OHIP employee at OHIP, but does not recall any specific cases. These inquiries all related to immigration investigations.

Constable A.J. MASON. Cst. Mason of the Orillia Detachment contacted OHIP for enrolment data as an investigational aid in attempting to locate a subject. The Barrie office of OHIP was contacted at telephone number 726-0326. Cst. Mason spoke to whoever answered the phone but does not know the person's name. Cst. Mason made a number of contacts with OHIP in the following investigations during 1975 and 1976:

(a) Immigration matter. Request for enrolment data as an investigative aid in attempt to locate. Obtained address but not beneficial in locating subject; (b) Immigration case. Contacted for enrolment data as investigative aid in attempt to locate. No information obtained from this source. (c) Income Tax tracer. Contact made for enrolment data as investigative aid in attempt to locate. Could provide no record of subject living at a particular address, but confirmed family with same surname living at that address. (d) Request for assistance in locating subject received from RCMP in British Columbia in connection with a charge of uttering forged documents. Contact made for enrolment data as an aid to locate. R.R.# obtained. Address found to be that of subject's parents. Information obtained did not assist in locating subject

of inquiry. (e) Investigation under the Family Allowance Act. Contact made for enrolment data as an aid to locate. Address obtained which enabled investigators to contact suspect, who was eventually charged under Section 338(1), C.C. for Fraud which involved the collection of benefits to which the subject was not entitled. (f) Request for assistance by Foreign Authorities. Contact made for enrolment data as an aid to locate. No information available regarding subject. (g) Applicant for civilian employment. In this particular case, enrolment data was not requested regarding the subject but was requested to determine an address for a reference provided in the application for employment. No address was available through OHIP.

. . . . .

Corporal B.S. MULDER. A former Investigator/Supervisor, Toronto Immigration and Passport Section, made two or three personal approaches to the OHIP office in Toronto. He does not recall the names of persons contacted but did make several later checks by telephone, the last time being about five years ago. Cpl. Mulder would identify himself as a member of the RCMP and supply an OHIP number if he had it, and other information for the purpose of updating the address of the subject of his investigation. These cases all related to immigration; Cpl. Mulder could not recall any specific cases or the name of the person contacted at OHIP.

Constable G.J. MARTELL. Cst. Martell of the Toronto Drug Section contacted the OHIP office through telephone number 482-1111 in Toronto on January 13, 1976, but cannot recall with certainty to whom he spoke. He does have the name of an OHIP employee recorded in his telephone directory. This was a Narcotic Control Act investigation regarding a subject. Cst. Martell wanted to determine if the subject actually existed

and, if so, obtain an address for him. No information was received from OHIP.

Corporal P. McGrath. Cpl. McGrath of Toronto Commercial Crime Section was conducting an assistance arson investigation and was attempting to locate a subject. On February 15, 1977, Cpl. McGrath telephoned the OHIP office at telephone number 965-8233 and enquired if they had any record of the subject. Cpl. McGrath did not ask for any specific individual but recalls that he spoke to a particular OHIP employee who was unable to provide any information.

Constable L.L. Nolan. Cst. Nolan made four inquiries of OHIP employees all in 1977. The RCMP was concerned about two organizations in Canada which appeared to be dominated by individuals who may be prone to acts of violence; it learned of a person who appeared to be associated with both organizations about whom little was known. Cst. Nolan contacted an OHIP employee in August 1977 by telephone, who knew him as a member of the RCMP; he requested enrolment data on the subject; approximately a week later the OHIP employee telephoned back to Cst. Nolan and advised that no information about the subject could be found. Some time in August or September, 1977 Cst. Nolan contacted the same OHIP employee with respect to a request from an RCMP Detachment outside Ontario that was investigating certain violence prone individuals who were members of an organization in western Canada. Cst. Nolan was asked to provide information about a particular individual who was alleged to have resided in Ontario at an earlier time. Cst. Nolan contacted the OHIP employee in August or September 1977 to obtain enrolment data with a view to confirming the identity of the subject and furnished the name of the subject and spouse. Shortly after that the OHIP employee contacted Cst. Nolan and advised that an individual by that name had been covered by OHIP under the family name of the subject's spouse but that the OHIP file had

been closed about four years previously. Cst. Nolan contacted the same OHIP employee in September, 1977 to determine as a general question unrelated to any individual or case whether in principle it would be possible to determine from OHIP records whether a person suffered from any particular medical condition (none specified) and was told that only the person's doctor had such information. The RCMP was informed by a friendly foreign intelligence service that a suspected espionage agent of a hostile foreign intelligence service was employed at one of two foreign business-oriented organizations in Ontario. Cst. Nolan contacted an OHIP employee in September or October, 1977, by telephone and asked whether it was possible to retrieve from OHIP records a list of the names of these two business organizations and was told that it was not.

Constable M.G. O'MALLEY. A former Toronto Immigration and Passport Section Investigator. Cst. O'Malley first spoke to an employee at OHIP at telephone 482-1111 in Toronto, who referred Cst. O'Malley to a second employee at OHIP in the Group Plan Department. He believes the person he spoke to was the second employee but does not actually recall whom he spoke to. He has also had contact with a third employee at OHIP about 4 years ago. He believes he was also referred to this third OHIP employee by the first OHIP employee. His reason for contacting OHIP was solely to determine a subject's current address and present employer. Cst. O'Malley cannot recall the case he was working on or if he obtained the information. These inquiries all related to immigration investigations.

Constable W.M. PYE. A former Toronto Immigration and Passport Section Investigator, Cst. Pye made contact with an employee at OHIP. He would identify himself as a member of the RCMP and request information on recent addresses of the person he was investigating. The inquiries all related to immigration investigations. He recalls one

specific case regarding a subject; an Immigration Inquiry, in which he was attempting to locate the subject. The OHIP employee supplied Cst. Pye with two possible persons with the subject's surname and addresses for both. Cst. Pye, after checking, determined that neither of these names supplied by OHIP were the ones he was looking for. The subject was never located.

Constable P. PAUW. A former Toronto Immigration and Passport Section Investigator, Cst. Pauw contacted OHIP by telephoning 482-1111, extension 220 and asked for a particular OHIP employee. However, if that employee as not available, he spoke to whoever answered the telephone. He would request information on the residence and the employer addresses of subjects under investigation. He could not recall any specific case with respect to his OHIP inquiries, all of which related to immigration investigations.

Constable A.F. PHILLIPS. Cst. Phillips presently stationed with the Windsor Commercial Crime Section, contacted the Windsor OHIP office at 1427 Quelette Ave., Windsor, Ontario, telephone number 258-7560 in September, 1977. He does not know the name of the OHIP employee he spoke with. This was an Income Tax investigation and the information requested was to determine whether a subject was paying OHIP premiums, the amount of monthly payment, and how long the subject was on file with OHIP. This information was received. No other information was obtained except the name of his doctor. The doctor was not contacted.

Constable T.P. PERRAULT. Cst. Perrault, while stationed on the London Drug Section, contacted an employee at the London OHIP office in February, 1978. Cst. Perrault wanted to establish whether an OHIP number and name coincided. OHIP did not confirm and provided no information.



Constable G.M. PYKE. Cst. Pyke of the Toronto Customs and Excise Section telephoned OHIP and believes he spoke to a specific OHIP employee in April, 1976. Cst. Pyke was investigating a subject under the Customs Act and wished to establish the residency in Canada of the subject. Enrolment data was received from OHIP which assisted in establishing the subject's residency in Ontario and partly as a result a vehicle was seized under the provisions of the Customs Act.

Constable C. REID. Presently a Toronto Immigration and Passport Investigator. Cst. Reid made contact with OHIP numerous times by telephone. His initial contact was with one OHIP employee at telephone number 482-1111 and more recently with a second OHIP employee at telephone number 965-8353 or 8357. Cst. Reid always asked for one of these two employees by name when calling but never met them personally. His purpose in calling OHIP was to obtain the employer's name and residence address of the subject of his investigation. On one occasion, his inquiry concerned an investigation where he found several OHIP numbers recorded on a piece of paper during an investigation and requested corresponding names. Cst. Reid could not recall specific cases or names. The inquiries all related to immigration investigations.

Constable I.H. ROGERS. Cst. Rogers, a former Toronto Immigration and Passport Section Investigator, contacted OHIP by telephone at 965-8325 and talk to whoever answered the telephone. He would identify himself as a member of the RCMP and request information on residence and employer's addresses. He does not recall any specific cases or the names of the persons contacted at OHIP. These inquiries all related to immigration investigations.

Constable D.E. RAMSAY. While employed with Toronto Customs and Excise Section from July, 1974 to August, 1977, Cst. Ramsay

obtained information concerning the address of subjects he was investigating by calling OHIP. The inquiries were directed to an OHIP employee, telephone (416) 482-1111. Cst. Ramsay does not recall any specific cases.

Corporal K.C. ST. GERMAIN. A former London Detachment member, Cpl. St. Germain advises that he contacted OHIP personnel in London by telephone but cannot recall the person or persons contacted. The contact was for the purpose of confirming addresses of subjects under investigation. Cpl. St. Germain could not recall specific cases. These inquiries all related to immigration investigations.

Corporal J.D. TAIT. Cpl. Tait, previously stationed with the Hamilton Detachment Immigration and Passport Section, recorded the name of an OHIP employee in his personal book. In connection with both Income Tax investigation and general investigations he contacted this employee for address and birth dates of people under investigation. No specific cases could be recalled and his last contact with this OHIP employee was about five or six years ago.

Constable B. WINTERS. Cst. B. Winters, while stationed at Mississauga Detachment on the General Investigation Section, advises that any request for information from OHIP records was made in reference to enrolment information only. These inquiries were made in reference to General Investigations. Cst. Winters is unable to recall any specific case. The person at OHIP was always contacted at telephone number 482-1111.

I turn now to a discussion of what has become known as the Riddell affair. In 1969, John Perry Riddell became a full time worker for the League for Socialist Action. In his evidence Mr. Riddell gave the following description of that organization:

The League for Socialists Action is an association of working people in Canada, whose goal is to achieve a society where

production is for human need and not for private profit. We think that is a goal of equalitative extension of democratic rights. It includes the defence of the rights we have now and their extension through society. We think that this will be achieved through the struggles of working people as a whole, rather than merely through our efforts and we support and participate in all the activities of working people for example, then and today, in supporting a struggle for Quebec Independence, or at that time and today, in trying to end U.S. aggression against Vietnam, and many other things.

Mr. Riddell testified that the youth organization associated with the League for Socialist Action was the Young Socialists and that it was fairly described as a Trotskyist organization which was a member of the Fourth International, an organization of about 50 or 60 groups in different countries of the world. Mr. Riddell expressed the opinion that it would be objectively unreasonable for an outsider, unfamiliar with the details of the evolution of Marxist thinking, to conclude that anyone belonging to a Trotskyist organization and who was a member of the Fourth International, belonged to an organization whose members believed in the violent overthrow of the existing government. I do not regard this opinion as objective or even valid. For the purposes of the discussion that follows, I assume that it is, indeed, objectively reasonable to perceive of the Young Socialists as an organization whose members believe in the violent overthrow of the existing government. To put it another way, I do not believe that it would be unreasonable for the service charged with the responsibility for the national security of this country so to look upon such a political organization.

In 1969 and 1970, Mr. Riddell visited a psychiatrist on five occasions. Evidence to this effect was given at one of our public hearings with Mr. Riddell's express consent. I would not have permitted evidence of this nature to be given at a public hearing unless I was satisfied that it was with the genuine approval of the individual whose privacy might be offended by the disclosure. In September, 1972, Mr. Riddell received an unsigned letter in an envelope post-marked Toronto and addressed to him at his residence. The letter read as follows:

COMRADE:

We have been most disturbed lately by indications of increasing emotional instability on your part, witnessed by psychiatric consultations, violent outbursts of temper and frequent periods of irritability. We note too from the enclosed letter that your condition has not escaped the notice of others. It is unfortunate that the author of the letter didn't see fit to forward it so that by now you could have taken steps to correct the situation.

No doubt the numerous responsibilities which have fallen upon your shoulders at this critical time in our history have played a large role in the development of your condition. While a certain amount of nervous strain is natural, and perhaps unavoidable, we do not feel that your recent behaviour is consistent with one who is capable of maintaining a responsible, sound leadership over our movement.

However, in consideration of your record of devoted service on our behalf, and in the best interest of the movement as a whole, we encourage you to lay bare the truth about your condition before the membership at the forthcoming YS Convention. An honest and open confession would do much to restore confidence in your sincerity and sense of responsibility. Should you fail to take this opportunity however, then in fairness you must be warned that we would consider it our duty to inform all comrades of the situation, an act which would not be extremely palatable to either party concerned.

Mr. Riddell's reaction to this communication was one of surprise. The Young Socialists, to his knowledge, had no history of distributing unsigned material. Mr. Riddell believed that only his wife and psychiatrist knew that he had visited a psychiatrist. He was astonished that information about these visits had found its way into this unsigned letter. Mr. Riddell assumed that the letter had originated with the police.

During the year 1972, a debate raged which divided the membership of the Young Socialists upon philosophical lines and which revolved around the question whether it was appropriate for the Young Socialists to encourage its members to become involved in the New Democratic Party.

In September, 1972, a second unsigned letter was circulated among the members of the Young Socialists. That letter read as follows:

LOYALTY TO THE INTERNATIONAL MEANS ABOVE ALL  
IN PRACTICE LOYALTY TO ITS CANADIAN SECTION

Comrade, the above statement was made in 1971 by John Riddell. His words imply that our loyalty to the Fourth International is second to our allegiance to our national movement, a very firm and decisive gesture on his part. And yet, for one so demonstrably dedicated to our cause in the past, certain of comrade Riddell's more recent actions raise questions in the minds of the writers as to the true direction in which sympathies lie. We make no accusations, but simply express our curiosity and concern over these actions, hoping that we will elicit a satisfactory response. We consider it incumbent upon all of us to demand frank and honest answers to these very serious questions, so that we may truly know the man who will determine our future in the days ahead.

Comrade Riddell, as our representative to the United Secretariat, could you please explain your conspicuous silence, during a time when we and our American comrades have been bitterly assailed on all sides by the majority of the International, including members of the United Secretariat itself, over the issues surrounding the rash and adventurous acts of the Latin American comrades?

Why did you stand by and allow this criticism to encourage the divisive and reactionary activities of the Tendency, activities which no doubt played a large role in prompting comrade Dowson, a man who



had devoted his entire life to the movement, to resign?

What are your true views on the question of armed struggle in revolutionary doctrine, bearing in mind the obvious implications of your silence on this issue?

Why have you neglected to make these views known to us and to those ultra-leftists who would destroy everything which we have attempted to build over the years?

Did you play a hand in an alleged invitation to prominent members of the United Secretariat to attend our National Convention?

What purpose would their presence serve? Perhaps you hope it would be interpreted as a sign of international solidarity on your behalf in order to buttress your position.

How would you reconcile the support of this group, which has actively criticized us and encouraged dissent in our ranks, with the true interests of the Canadian section?

How do you explain a remark made recently in which you flatly accused comrade Dowson of attempting to destroy the movement by using obstructionist tactics?

What are your views on freedom of discussion within the movement, particularly in light of your outburst during a disagreement with a comrade over what those privy to the conversation considered to be a rather nonsensical point? Do you feel that telling someone that if he insisted on disagreeing he could "get out" of the movement is consistent with the democratic principles which are a cornerstone of our philosophy?

In view of your well known close relationship with the IMG, what are your views on its encroachment in our affairs through its active support for the Tendency?

AND NOW, HERE ARE SOME QUESTIONS FOR CONSIDERATION BY ALL COMRADES!

Would it not be to the advantage of the majority of the International to have placed in power in Canada a man considered sympathetic to their views on revolutionary strategy?

Does a person with a sense of loyalty remain silent when one who has supported him, and indeed nominated him as his successor, is criticized and abused?

Does a man of reason violently and irrationally assail one who dares to question his views?

Does a courageous person allow his colleagues to be belittled and chastised without coming to their defence?

Does a true Trotskyist allow his principles to be perverted by a gaggle of opportunistic revisionists?

COMRADE, WE IMPORE YOU TO JOIN WITH US IN DEMANDING ANSWERS TO THESE QUESTIONS, AND MANY OTHERS WHICH PLAGUE THE WRITERS' MINDS, BEFORE WE DECIDE IN WHOM WE ARE GOING TO ENTRUST THE FUTURE OF OUR MOVEMENT IN CANADA. TO THOSE WHO DOUBT THE INTENTION OF THIS DOCUMENT WE SAY, WHAT DOES COMRADE RIDDELL HAVE TO FEAR FROM QUESTIONS TO WHICH HE MAY REPLY HONESTLY AND OPENLY? IF HIS ANSWERS ALLAY OUR FEARS, SO MUCH THE BETTER. BUT WE CONSIDER THE IMPLICATIONS IN HIS ACTIONS TOO SERIOUS TO BE IGNORED. NEVER FEAR THE TRUTH COMRADES, FOR IT IS BY OUR ADHERENCE TO THE TRUTH THAT WE WILL ONE DAY REALIZE OUR GOAL!

In December, 1972, a convention of Young Socialists was held at King Edward School in Toronto. On the morning of the conference, when the gymnasium at the school was opened for the Young Socialists, copies of the following unsigned letter were found on all the chairs:

## COMRADES:

In recent months, it has become apparent to many that John Riddell is suffering from extreme emotional anxiety and instability. If the above statement is shocking, and incredible in your eyes, then we call to your attention numerous incidents involving violent and irrational outbursts of temper, and prolonged periods of depression and irritability which have marked comrade Riddell's behaviour throughout the past few weeks. Looking on all those close to him with deep suspicion, he accuses them of deserting him, and of attempting to undermine his authority. Such behaviour becomes even more frightening when considering that in the past he has been forced to seek psychiatric aid as a solution to this problem.

At this point in our history, when we are threatened by the divisive forces of the Tendency, and criticized on all sides by the agents of opportunism and reaction, it is more important than ever that we have as our leader a man capable of remaining calm in the face of stress and pressure. And yet comrade Riddell displays an inability to cope with the responsibilities of leadership; instead as each day goes by he becomes more and more irrational. In our opinion his character of late is not consistent with our ideals of leadership, and we fear for the future of our movement.

At this point it should be noted that we approached comrade Riddell and asked him to make a full and open confession of his condition to everyone at this convention. This he refused to do, thereby illustrating both a desperate desire to cling to power at all costs, and a basic dishonesty in his dealings with all of us. The seriousness of this problem is too great to be ignored comrades. What we have described is not rumour, but fact, and based on this must be your decision to consider very carefully our choice of leaders, in the greater interests

of our movement, and all we are hoping to achieve.

The letter distributed at King Edward School attempted to use accurate health information to sow dissension, disruption and distrust among the members of the Young Socialists. The three letters were written and distributed by the RCMP. Superintendent Ian William Taylor testified that, in 1972, the RCMP had been involved in an operation which required letters similar to those which I have recited above to be written. He expressly admitted that the letters addressed to Mr. Riddell and the letter distributed at the King Edward School were written by members of the RCMP with the authorization of senior RCMP officers and that there were, in fact, copies of these letters in the RCMP file.

Superintendent Taylor said that the RCMP file was classified "Top Secret" but that an examination of the file disclosed that the health information in question did not come from a physician, physician's employee, health-care worker, hospital employee, or any other person under a duty to preserve confidentiality under Ontario legislation. I was permitted to read the file, and did so. My study of the relevant documents in the file caused me to conclude that Superintendent Taylor's evidence that the source of the health information in the letters was not a person under a duty to keep such information confidential was entirely accurate.

It has been submitted that I should recommend legislative changes that would give access to confidential health information in the possession of OHIP to the RCMP to aid their members in the discharge of their police functions. Elsewhere in this report I recognize the public interest in allowing the police in general the right to more information than they are now entitled to obtain. With respect to the RCMP, however, a force not answerable to provincial authorities, one cannot remain confident that OHIP information would not be used for such purposes as health information was used in the Riddell affair. I do not believe that the use of confidential information for these or similar purposes is acceptable to members of Ontario society. The incident itself, however, has disturbing implications.

The RCMP utilized accurate health information for disruptive purposes. Superintendent Taylor said that this was the only incident of its kind. By its very nature the Security Service of the RCMP is isolated from the rest of the force. Every member functions on a "need to know" basis only. Although I am satisfied that Superintendent Taylor believes his statement is accurate, I confess that I have serious doubts about its

accuracy. For one thing, given the structure of the Security Service, it is not the case that a given member's act of this kind would necessarily come to the attention of his or her superiors or, indeed, anyone else.

Another reason for my doubt about the accuracy of Superintendent Taylor's statement is to be found in our experience with the accuracy or reliability of statements made by the RCMP during our hearings. For example, part of our investigation involved an inquiry into certain allegations made in stories in The Globe and Mail written by reporter Lawrence Martin and in which he had asserted that the RCMP had used health information for disruptive purposes. Prior to February, 1979, no evidence supporting this assertion had come to our attention or was known to us. Mr. Martin, who was assigned to Washington by his employer, refused my request to return to give evidence and remained out of the jurisdiction and beyond my power to compel his attendance and his testimony. Mr. Strosberg summed up the status of the investigation when, at a hearing on January 16, 1979, he stated that,

There has been no evidence that medical information which was obtained by the RCMP was used in Ontario for disruptive purposes...and it is my submission to you... that the investigation does not show...the use of medical information for disruptive purposes.

. . . . .

One can only conclude that...the use by the RCMP of medical information, however obtained, for disruptive purposes either in Ontario or elsewhere, just did not take place. [emphasis added]

When he made these submissions, Mr. Strosberg was not aware of the Riddell incident. It is significant, however, that the RCMP, as a force, knew of the Riddell incident and the letters written by its members before December, 1978. It must have become aware of these letters after a written submission mentioning the letters was made to the McDonald Commission on January 18, 1978. Nevertheless, on January 16, 1979, immediately after Mr. Strosberg had made the statement recited above, Mr. Pennington, representing the RCMP and the Solicitor General of Canada, made the following submission:



...I would quite concur with the submission by Commission Counsel that there really is no evidence before you, Sir, that would suggest that there has been the use of any medical information from any source in Ontario that was used improperly by the RCMP. There just isn't, in my submission, a shred of evidence.

. . . . .

I know this Commission, which has been in existence for more than a year, has not received a single complaint from anybody that they were in any way humiliated or blackmailed or disrupted by the RCMP using medical information against them. [emphasis added]

Mr. Pennington's statement was made after I had been assured that I had had complete disclosure from the RCMP. The RCMP and the Solicitor General must have known that this representation was untrue. It was only after Mr. Strosberg had become aware of the existence of the Riddell incident and the letters, and had asked the RCMP to answer the express question whether the letters had been written by RCMP members, that it was admitted that the letters had originated with the RCMP.

In his testimony, Superintendent Taylor said that letter writing operations had been suspended pending the submission of the report of the McDonald Commission. It is therefore not certain that further operations of this kind will not be undertaken in the future. This gives rise to the concern I have already mentioned. If confidential health information were to be made available to the RCMP from OHIP records, even in a limited fashion, could there be any safeguard against its use for disruptive purposes? Superintendent Taylor expressed this opinion:

...if subsequently the Provincial Government passed in whatever manner was appropriate, enabling legislation and that it was very clear that any medical information would be provided for a specific person as us, excuse me, a specific reason and it clearly excluded this type of activity, I'm quite confident in my own mind and it's a personal view, that the medical information obtained pursuant to that legislation legitimately

would not be used for any purpose that was not permitted.

As I have said, given the present constitutional barriers, there exists no mechanism that could ensure that health information disclosed for legitimate police purposes to the RCMP would not be used for disruptive purposes or some other purpose not intended at the time of the disclosure. It seems quite clear that the provincial authorities are without the capability of following up and checking on the ultimate use of the information. The only check is the integrity and self-discipline of the RCMP itself. In a democratic society, no police force, no matter how generally well respected, should be allowed to be a law unto itself. To rely solely upon a police force's integrity and self-discipline is to permit that force to become a law unto itself.

Only if the RCMP, by federal-provincial agreement or otherwise, were first made accountable to a provincial authority for the information it was entitled to have, should any thought be given to allowing it access to provincially maintained health information for acceptable police purposes. One would want to reconsider this position if, in time, the security-service responsibilities were removed from the RCMP and entrusted to a separate organization or agency, leaving the force with its conventional police role.

## The Department of Manpower and Immigration

Contact with OHIP to obtain enrolment information was made as a matter of routine by employees of the Department of Manpower and Immigration, now known as the Department of Employment and Immigration and which, for convenience, I shall refer to as the Immigration Department. Michael Joseph Rafferty, an employee of the Toronto regional office of the Immigration Department, testified at our hearings. He became involved in immigration investigations in October, 1971. Before that date, immigration investigators had requested information from the Ontario Hospital Services Commission, OHIP's predecessor. Mr. Rafferty said that the origins of the practice have been lost in antiquity. The practice was probably informal at first. After OHIP's creation in 1972, a form letter, directed to OHIP requesting information, began to be used. The most recent form letter was addressed to John R. Harnett, the Director of Enrolment Services, and read as follows:

Dear Sir:

This Department is trying to locate the person named below. Would you please advise us if you have any record of the present employment and/or home address of this individual.

Your co-operation in these matters is greatly appreciated.

Yours very truly,

Immigration Officer  
for Officer-in-Charge  
Canada Immigration Centre  
480 University Ave.  
Toronto, Ontario  
M5G 1V2

Name: \_\_\_\_\_  
Date of Birth: \_\_\_\_\_  
Last known address: \_\_\_\_\_  
Last Known Employer: \_\_\_\_\_  
O.H.I.P. Number: \_\_\_\_\_  
\_\_\_\_\_

Reply:  
Present Address: \_\_\_\_\_  
Present Employer: \_\_\_\_\_

Mr. Rafferty attempted to determine the extent of the Immigration Department's contacts with OHIP. There were no statistics kept of the exact number of letters sent to OHIP or of the number of replies. His best estimate, after a detailed investigation, was that the frequency of requests varied from 25 to 100 per month and that, as an average, there were approximately 60 to 70 answers monthly from OHIP. The Immigration Department never sought or received health information from OHIP. The purpose for which OHIP was approached was to obtain current addresses, or employers' addresses of persons who were believed or known to be illegally in Canada, and thereby subject to inquiry action and possible deportation from Canada.

I find it significant that this form was directed to Mr. Harnett who, in 1972, became the Director of the Enrolment Branch of OHIP. He reported to the General Manager, Mr. Fetherston and was at the same level administratively, as

far as responsibility was concerned, as David M. Buchanan who was in charge of the Insurance Claims Branch. Mr. Harnett testified that prior to OHIP's creation in April, 1972, the policy of the Ontario Hospital Services Commission was to co-operate with, and disclose information to, the police and the Immigration Department. He produced minutes of meetings of the Ontario Hospital Services Commission held in 1960. The following are extracts from some of these minutes:

Minutes of the meeting of the Commission  
held on August 17th in Mr. Ogilvie's office  
commencing at 9:30 a.m.

. . . . .

1456 COMMISSION'S FILES - TRACING  
INFORMATION

Mr. Foster stated in a memo to Mr. Ogilvie that as a carry-over from Blue Cross operations, they consider information contained in their files to be confidential. Tracing information has traditionally been supplied only to hospitals and to recognized law enforcement agencies. Mr. Foster desired the confirmation of this policy by the Commission.

They had also received a request from the Department of Citizenship and Immigration that they provided with tracing information when other sources of information available to them are unfruitful.

It was agreed that the Commission files should not be available for anyone.

. . . . .

Minutes of the meeting of the Commission  
held on September 7th in Mr. Ogilvie's  
Office commencing at 9:30 a.m.

. . . . .

f) Commission's Files - Tracing Information  
(1456)

The record should read that it had been the practice to make Commission records

available only to law enforcement agencies and to hospitals. It was agreed that requests for information of this nature should be considered and dealt with by the General Manager at his discretion.

MINUTES OF DIVISION MANAGER'S MEETING  
Thursday, September 22, 1960

MANAGEMENT COMMITTEE

- a) The Commission had approved the continuing practice of providing information, available from our files, to hospitals and recognized law enforcement agencies, which would assist in tracing individuals. Further, the Commission had agreed that the General Manager should consider requests from other sources and deal with them at his discretion. The General Manager had agreed that The Department of Citizenship and Immigration was to be provided with such information upon their official request.

The provision of such information will require approval at the Division Manager level.

Despite the creation of OHIP by The Health Insurance Act, 1972 in April, 1972, and the language of the new legislation, Mr. Harnett did not cause the policy of disclosing this information to the police and the Immigration Department to be reviewed, let alone changed. Given his position in the Department of Health, as the Ministry was then called, Mr. Harnett ought to have known that to reveal information to the police and to the Immigration Department in the manner in which it was being done was a breach of section 44 of The Health Insurance Act, 1972. His position was made plain by the following exchange with Mr. Strosberg at our hearings:

Q. In 1972, did you become aware of section forty-four of The Health Insurance Act?

A. The particular portion relating to...

Q. Confidentiality? Yes, sir.

A. Confidentiality. I have to say that, no, I am aware of the wording, thank you. I



have to say that in my position as Director of the Enrolment Branch I certainly should have been aware of it, but I can't consciously say I was aware of it, of the exact content.

Q. Well, you said two things. The first is that you should have?

A. I should have.

Q. Are you saying, however, although you should have that you were not?

A. I think it boils down to a matter of awareness. I was aware then, let me say I must have been aware of that particular clause relating to confidentiality, yes.

Q. Did you ever really direct your mind to that section dealing with confidentiality before November of 1977?

A. No, sir. Actually that's what I meant by being not consciously aware of it.

Q. Before November of 1977, that's from the time OHIP was established until November of 1977, what did you believe that OHIP's policy was relating to the release of information?

A. To my mind, the administrative policy of OHIP in this connection was simply a carry forward from the policy that applied under the Ontario Hospital Services Commission.

Q. Was that to release information on request to the police?

A. And to the Department of Immigration.

Q. Did you ever have any discussions with for example Mister Fetherston prior to November of 1977 relating to the release of information to the Immigration Department?

A. I recall a conversation but I don't recall in what context it was made. It may

have been a passing remark but it was my understanding that...

Q. When did this conversation take place?

A. It's difficult to recall. I would say late 1976, for example.

Q. Yes, and where was this conversation at?

A. In Mister Fetherston's office, but it was not, I have to say that if memory serves at all that it was not a conversation that dealt specifically with the release of information to Immigration. It may have been a passing remark. It certainly wasn't my purpose in being in Mister Fetherston's office to inform him that information was being given to Immigration.

Q. What did you say during this conversation?

A. I don't recall off hand. I simply recall a conversation that we were providing information to Immigration.

Q. That was the substance of the remark that you made during the course of this conversation that your department was providing information to the Immigration Department?

A. That's correct.

Q. Did Mister Fetherston respond in such a way that you either, that you took it that he either thought this was proper or improper?

A. I believe Mister Fetherston understood that it was proper at the time, because we were still working under the same administrative policies that applied under OHSC.

Q. Do I take it then from this evidence that you are giving, sir, that you believe that Mister Fetherston knew before November of 1977 that your, that the enrolment part

of OHIP was giving information to the Immigration Department?

A. I think all employees of the Health Insurance Division were aware of this.

Q. That includes Mister Fetherston?

A. Yes, sir.

Q. Do you have any reason to believe that the, you reported to Mister Fetherston, Mister Fetherston reported to the assistant deputy minister, is that correct?

A. Correct. Correct.

Q. Who reported to the deputy minister who reported to the Minister?

A. Correct.

Q. Do you have any knowledge, information or belief that would lead you to a conclusion that the assistant deputy minister knew that it was a policy of OHIP to give information to the Immigration Department?

A. No, sir.

Q. Or the deputy minister?

A. No, sir.

Q. Or the Minister?

A. No, sir.

It is clear that Mr. Fetherston, the General Manager of OHIP, also knew in 1976 that biographical information was being given to the Immigration Department and did nothing to prohibit the practice. Mr. Harnett's handling of this matter was so routine that he delegated to his administrative assistant the responsibility of answering the 25 to 100 monthly requests for information from the Immigration Department.

Nor, as a matter of fact, was Mr. Harnett alone in his understanding that the policy of OHIP was to co-operate with the police. Mr. Buchanan, who, I have said was in charge of the

Insurance Claims Branch and was responsible for the claims processing in the district offices, testified that,

It was my responsibility and I accept the responsibility that [the employees at district offices] acted within the policy of the Plan, and the policy as far as enrolment information was concerned was that it could be given to the police.

This policy was, as he put it, given to him by the General Manager, Mr. Fetherston. By his own admission, Mr. Buchanan was aware of section 44 of The Health Insurance Act, 1972 at the time:

Q. Did it occur to you that the policy as to the release of information to the police as given to you was in conflict with section 44 of The Health Insurance Act?

A. To be perfectly frank, it didn't.

. . . . .

Q. Did you consider the problem as to whether or not [to release information to police] was in conflict with section 44 when this policy was given to you?

A. No, I didn't.

One can say, therefore, that the three senior executives at OHIP, Messrs. Fetherston, Harnett and Buchanan formulated or accepted an administrative policy of disclosing information to the police and the Immigration Department in breach of section 44 of The Health Insurance Act, 1972 without considering whether this policy could be reconciled with the language of section 44 of The Health Insurance Act, 1972. If they had simply addressed themselves to this question they would have immediately concluded that it could not.

Under the Ontario Health Insurance Plan, certain health-care providers are paid a fee for services rendered in accordance with prescribed fee schedules. Payment is the result of a process commenced by the submission of a claim by a health-care provider to OHIP for payment. OHIP, of course, must ensure that no health-care provider defrauds the Plan. A monitoring branch was therefore established. From time to time OHIP found it

necessary to involve the police in investigations of suspected fraud.

In February, 1973, an informal agreement was reached between the Ontario Provincial Police and the Metropolitan Toronto Police Force which divided jurisdiction for the investigation of suspected frauds. Those suspected of having occurred within the Municipality of Metropolitan Toronto, it was agreed, would be investigated by the Metro Police and those suspected of having taken place elsewhere in Ontario would be investigated by the Anti-Rackets Branch of the OPP. Under the normal procedure, a written request issued from the offices of Dr. Gerald Gold, then of the Physician Service Monitoring Branch of OHIP, to the Director of the Anti-Rackets Branch who assigned the investigation to the members of his staff. The majority of the suspected frauds investigated were of physicians, laboratories or individuals thought to be making improper claims for reimbursement for services allegedly rendered. Accompanying the requests for the investigation were all relevant materials including copies of physician claim cards containing particularized health information in the form of a diagnostic code.

As I have already pointed out, section 44(1) of The Health Insurance Act, 1972 creates an obligation of confidentiality. Because of its importance, I set the subsection out again.

Each member of the Medical Review Committee, every practitioner review committee, the Medical Eligibility Committee and the Appeal Board and each employee thereof, the General Manager and each person engaged in the administration of this Act and the regulations shall preserve secrecy with respect to all matters that come to his knowledge in the course of his employment or duties pertaining to insured persons and any insured services rendered and the payments made therefor, and shall not communicate any such matters to any other person except as otherwise provided in this Act.

Exceptions to this general obligation of confidentiality permit the release of some information. One exception relates to police investigations and another to the administration of the Act. These exceptions are found in subsection 44(2)(a) and (b) as follows:

(2) A person referred to in subsection 1 may furnish information pertaining to the



date or dates on which insured services were provided and for whom, the name and address of the hospital and health facility or person who provided the services, the amounts paid or payable by the Plan for such services and the hospital, health facility or person to whom the money was paid or is payable, but such information shall be furnished only,

(a) in connection with the administration of this Act, The Medical Act, The Public Hospitals Act, The Private Hospitals Act, The Ambulance Act or the Hospital Insurance and Diagnostic Services Act (Canada), the Medical Care Act (Canada) or the Criminal Code (Canada), or regulations made thereunder;

(b) in proceedings under this Act or the regulations;

An examination of these provisions makes it clear that it is perfectly proper for OHIP to release to the police the type of information described in section 44(2) in connection with a fraud investigation. However, even in the case of a proper police investigation of suspected fraud, because of the language of section 44(2), OHIP is not permitted to furnish particularized diagnostic information.

In 1973, the Toronto District office of OHIP was located at 15 Overlea Boulevard, in what is now the Borough of East York. In May, 1973, Detective Sergeant Melvyn Roy Stroud of the OPP and Constables Kendrick and Savage, were investigating suspected fraud against OHIP. They were given office space at 15 Overlea Boulevard. An OHIP employee acted as a liaison officer and was assigned the responsibility of obtaining any information that was necessary from the OHIP system for these officers. This was the origin of the practice of assigning office space within the confines of the OHIP offices to the OPP and Metro Police. In October, 1973, the Toronto District Office was moved to 2195 Yonge Street in Toronto. Donald McLean was the Director of the Toronto District Office from OHIP's inception and had primary responsibility for this move. Mr. McLean decided to provide accommodation for the police at 2195 Yonge Street. This was done at Mr. McLean's direction without any express or implied authorization from his superiors. At first, the police office was located on the fourth floor at 2195 Yonge Street but it was

changed to the third floor in 1976. Coincidentally, in October, 1973, at the time of the move to 2195 Yonge Street, the person acting as liaison officer retired. No other OHIP employee was assigned the task of liaison officer and the police were given direct access to all OHIP information they needed.

The police office was a secure area. Only the OPP and the Metro Police had keys to this office. There was no system which required police officers to identify themselves upon entering or leaving the OHIP premises. Both the OPP and the Metro Police used this police office, as Mr. McLean said, from time to time until about September, 1977. This access and use is illustrated by the activities of Sergeant Brian King of the Metro Police. He used the office at 2195 Yonge Street for approximately four months in 1974 and at periodic intervals thereafter until 1977. He had a key and unrestricted access to this office. In fact, in the fall of 1977, he attended at 2195 Yonge Street on one occasion simply to use the telephone in the office. At the time of our hearings, he no longer had the key. He could not remember to whom he gave the key although he thought it was a fellow Metro Police officer. He was certain that he had not given it to an OHIP employee.

Police officers were permitted access to all OHIP records including claims reference microfiche and enrolment microfiche. No logs or records of access were kept. In short, the OPP and Metro Police were given complete access to all OHIP's information. Neither internal OPP and Metro Police investigations nor our careful and independent investigation disclosed any occasion upon which an OPP officer or Metro Police officer exploited this police office and the access to OHIP records by obtaining any information for any other use than that of a fraud investigation. This loose and intimate relationship, however, would raise an apprehension in the mind of a reasonable person that the police could, at will, obtain the health information of any person in the Province, for, as I have said, the Toronto District Office (and every other OHIP District Office) maintained a complete set of microfiche containing the complete health history of all OHIP subscribers and their dependants.

Fraud against OHIP cannot be tolerated. The OPP and Metro Police forces must be permitted to have access to information for the purposes of investigating suspected frauds. Nevertheless, it is unreasonable to permit any police force, either in fact or in appearance, unlimited and unrestricted access to the health information maintained by OHIP which is health information about almost all residents of Ontario.

In Windsor, the OPP Intelligence Unit required additional space. The Ministry of Government Services located this Unit adjacent to part of the OHIP offices on the second floor of the building at 1427 Ouellette Avenue. The OHIP office "wrapped around" the OPP office to the west and south. The fire exit from the OPP office entered into the OHIP office proper. In Windsor, before November, 1977, the claims reference microfiche and enrolment microfiche were in an unlocked room on this floor. The police officers had free and complete access to the OHIP office on the second floor simply by opening the fire door at the south end of the OPP office. The OPP officers normally used this exit at night as a means of access to the washroom. When this door was opened the officers were within the OHIP office and within steps of the microfiche. I am satisfied that at no time did members of the OPP carry out any unauthorized reviews of the OHIP microfiche. But, again, the circumstances can reasonably justify the apprehension that the OPP could obtain access to the health information of any OHIP subscriber or his or her dependants at will. Such proximity should not be permitted.

*Recommendation:*

14. *That all necessary steps be taken to separate accommodation for the police from OHIP facilities.*

It is clear that neither the Minister nor the Deputy Minister had knowledge of the existence of the police office at 2195 Yonge Street. When W. Allan Backley, then Deputy Minister of Health, learned of the existence of this office from Mr. Strosberg, he was surprised, if not shocked. It was his view that the OPP and Metro Police ought immediately to vacate the OHIP premises. The existence of this police office at 2195 Yonge Street is another example of the failure of OHIP employees to disclose relevant information to us during the inquiry. It was Mr. Strosberg and Miss Smith, our counsel and associate counsel, who discovered the office. It is significant that the office's existence was not disclosed to our investigators who had attended at 2195 Yonge Street and carried out intensive interviews with employees on several occasions. Mr. McLean gave no satisfactory explanation for his failure to advise us of the office's existence. To him it simply did not seem significant.

From time to time, the OPP, the Metro Police and other police forces in Ontario obtained or attempted to obtain information from OHIP by direct request to OHIP employees without patient authorization and in connection with matters other than

fraud investigations. The circumstances of some of these contacts follow.

Detective Sergeant Melvyn Roy Stroud of the OPP contacted OHIP on five occasions. It will be enough to refer to two of these cases. In January, 1977, Detective Sergeant Stroud was asked by Detective Inspector Gibson to obtain information from OHIP. Detective Inspector Gibson was investigating a homicide and was attempting to determine whether or not a certain physician had prescribed a chloroform drug for a suspect. This information was believed to be relevant to the investigation because chloroform had been used in a homicide. Detective Sergeant Stroud contacted an OHIP employee but was unable to determine whether a drug of that kind had been prescribed. In October, 1977, Detective Sergeant Stroud was contacted by an officer from the OPP detachment at Newcastle who was attempting to locate an arson suspect. Detective Sergeant Stroud contacted an OHIP employee who provided him with the names and addresses of all persons with names similar to that of the suspect.

It is significant that members of the OPP contacted Detective Sergeant Stroud and requested him to obtain this information from OHIP. They did so because they were aware that he was familiar with the OHIP system and had worked on OHIP fraud investigation. They rightly concluded that it would be easier for him to obtain information from OHIP because he had developed a personal relationship with OHIP employees.

Detective Sergeant Ronald Brian Roberts of the OPP had also been involved in OHIP investigations. On several occasions he had been asked by other OPP officers to obtain information, without patient authorization, from OHIP. On one occasion, in the fall of 1976, he was successful in obtaining from OHIP the residence or place of employment of a suspect in a murder investigation. On two other occasions in early 1977, Detective Sergeant Roberts was given OHIP numbers by OPP officers who were involved in an investigation relating to forged cheques. It appears that OHIP numbers had been used as a means of identification by persons cashing forged cheques. The purpose of this investigation was to establish whether the person cashing the cheque had used a correct name or a false name and a proper OHIP number. If the OHIP number had been a valid subsisting number, the OPP would have been in a position to approach the subscriber to determine whether he or she was the person who had cashed the cheque or whether his or her OHIP card had been stolen.

Nor was Detective Sergeant Roberts the only police officer in Ontario to contact OHIP because OHIP numbers had been used for identification. Sergeant Gordon Brian Howe, of the



Hamilton-Wentworth Regional Police Department, in February, 1975, was investigating a fraud relating to stolen government cheques which had been cashed using an OHIP number as identification. It is often the case that, when a person wishes to cash a cheque at a store or a bank, his or her driver's licence number, social insurance number or OHIP number is noted on the back of the cheque. Sergeant Howe contacted Mr. Board of OHIP's Hamilton District Office to determine whether the OHIP number was genuine and, if so, the most recent address according to OHIP's records. He approached Mr. Board on five or six occasions to obtain this type of information.

Deputy Chief James Noble of the Metro Police testified that the members of his force had been canvassed to determine the extent to which they had contacted OHIP. It was common practice for the Metro Police to approach OHIP in fraud investigations relating to forged cheques in respect of which OHIP numbers had been given as a means of identification. The information required from OHIP was, as in Sergeant Howe's experience, whether the OHIP number was valid and, if so, the most recent address of the person whose number had been used. Deputy Chief Noble said that in 1977, the Metro Police had received 15,745 arrest warrants for Criminal Code offences. Every division selected a senior constable to attempt to execute many of these warrants. This officer, called a warrant officer, develops his or her own technique for the execution of these warrants. Occasionally, one of the warrant officers attempted to determine the most recent address if he had an OHIP number. It appears that the warrant officer did not appreciate that OHIP maintained a set of alpha microfiche, which is an alphabetical listing, by subscriber, showing either the home address, in the case of a pay-direct subscriber, or the employer's address, in the case of a group. Access to these microfiche would have obviously facilitated the execution of these warrants.

In June, 1976, Sergeant Stanley Gayler, of the Metro Police, approached an OHIP employee regarding someone who was listed as a missing person and who was also wanted in connection with two arrest warrants. Sergeant Gayler wanted to determine whether the person sought was a paid up subscriber and his current address. OHIP had no information. Apparently the file was dormant because the person had ceased to be a paid up subscriber.

On June 9, 1978, a Sergeant Mantle of the Metro Police was involved in the preparation of a brief for an inquest into the death of a person who had died from an overdose of menthol. Sergeant Mantle had information that, prior to his death, the deceased had been treated by two identified physicians. He



contacted OHIP in an attempt to find the names of any other physicians who had treated the deceased in the relevant period in order to determine whether or not they should be asked to testify at an inquest.

On December 23, 1977, Metro Police Constable McGarvey found a purse containing an OHIP card, but no other identification. The officer contacted OHIP in an attempt to determine the address of the owner of the purse.

On August 31, 1977, a body was found floating in the Toronto harbour. Metro Police Sergeant Ludlow discovered an OHIP card in the deceased's wallet. He telephoned OHIP in an attempt to obtain an address for the deceased so that he could locate relatives to have the body identified.

On April 23, 1975, Metro Police Staff Sergeant Newsome, who was a member of the homicide squad, was assisting in the investigation of a person who had been reported missing on May 1, 1974. In an attempt to determine whether foul play was involved, he contacted OHIP to determine whether or not the missing person's OHIP number was active.

On one occasion, an OPP officer found the body of an infant near Thunder Bay. The OPP contacted OHIP to attempt to determine the names of persons who had given birth within a specified period. They were unable to secure this information.

OPP Chief Superintendent Robert Archie Ferguson testified that a survey of all OPP members had been carried out to determine the extent and the circumstances of any contacts by OPP officers with OHIP. The search was not exhaustive because in the period of 1972 to the fall of 1978, there were approximately 600 officers who could not be canvassed for such reasons as death and retirement. Nine individual officers had a recollection of obtaining enrolment information from OHIP during police investigations for purposes similar to those outlined above.

The inescapable conclusion from the evidence is that the OPP, Metro Police and other municipal police forces, from time to time, attempted to obtain, and on some occasions, received both health and enrolment information from OHIP records in circumstances which did not permit them to have the information under section 44 of The Health Insurance Act, 1972. The information obtained was used only for legitimate and proper police purposes. Neither the OPP, the Metro Police nor any other municipal police force in Ontario used any information obtained from OHIP for purposes of disruption, intimidation or blackmail or any other improper or illegal purposes. Moreover, the further

allegation that the police had obtained information from OHIP from paid informants is without foundation.

OHIP was created as a means of providing universal health insurance for residents of Ontario. The Plan must maintain certain personalized health information to permit it to function properly and to facilitate the auditing of the billing practices of health-care providers. For these reasons, information concerning patients' treatment and conditions must be disclosed by health-care providers to OHIP. This disclosure is authorized and, indeed, required, by section 33 of the Act which provides as follows:

33. (1) Every physician and practitioner who performs an insured service for an insured person shall provide the insured person, or the General Manager, with the particulars of his services and account that are required by this Act and the regulations or the General Manager for the purpose of payment of the claim.

(2) Every insured person shall be deemed to have authorized his physician or practitioner who performed insured services to provide the General Manager with such information respecting the insured services performed as the General Manager requires for the purposes of the Plan.

(3) No action lies against a physician, practitioner, hospital or related health facility providing insured services or any member of his or its staff because of the furnishing to the General Manager information relating to insured services provided by him or it.

OHIP was not established to create a pool of information easily accessible to the police. It is in the public interest to maintain the privacy of patients and the confidentiality of health information in OHIP's possession both because a person covered by the Plan has no alternative to having information about him or her forwarded to OHIP and because it is important that health-care providers candidly disclose to OHIP diagnostic and fee schedule codes necessary for the purposes of payment and auditing. Enrolment information, that is, an individual's name, and residence or his or her employer's name and address, is not health information. In our society, one's home address, the

name of one's employer and his, her or its address are not generally considered private or intimate matters. One's home address is normally easily obtained by others by examining the telephone directory or municipal directory or by making a motor vehicle search or a licence search in the Ministry of Transportation and Communications.

The evidence before me indicates that the RCMP, OPP and municipal forces, for such legitimate purposes as locating someone, would be assisted by having access to OHIP enrolment information. It is surely in the public interest to make this part of police work easier. Moreover, it is hard to see how any legitimate interest would be prejudiced. In my opinion, the Immigration Department has also demonstrated a legitimate need for this information.

This point of view seems to me to be reflected in recent social legislation. The Family Law Reform Act, 1978, S.O. 1978, chapter 2, provides a mechanism by which the Court may make an order permitting one to learn or confirm the whereabouts of a person against whom an order is sought to be made by giving access to information in the possession of a public agency. The provision is found in the following section:

26. (1) Where it appears to a court that,

- (a) for the purpose of bringing an application under this Part; or
- (b) for the purpose of the enforcement of an order for support, custody or access,

the proposed applicant or person in whose favour the order is made has need to learn or confirm the whereabouts of the proposed respondent or person against whom the order is made, the court may order any person or public agency to provide the court with such particulars of the address as are contained in the records in its custody and the person or agency shall provide to the court such particulars as it is able to provide.

(2) This section binds the Crown in right of Ontario.

In a recent case, Gordon v. Gordon (1978), 1 F.L.R.A.C. 1, Judge W.E. MacLatchy, of the Provincial Court (Family Division)

of the Judicial District of York, had to decide whether this section conflicted with section 44 of The Health Insurance Act, 1972. His reasons for judgment read, in part, as follows:

One argument put forth on behalf of the Ministry of Health was that they had a specific direction given to them by the Act under section 44, that they were to keep secret all matters that come to his knowledge in the course of his employment and shall not communicate any information to any other person except as otherwise provided in the Act. Subsection 2 does provide that information shall be furnished ONLY and then it provides certain circumstances as set forth in the said subsection. This then deals specifically with information concerning those persons who are insured under OHIP. It is clearly understood why such a provision was made and that is that any and all information concerning one of their subscribers should be kept in strictest confidence. It would be an unfair advantage to be taken by a litigant or other person against the subscriber to be provided with the information that in fact, the subscriber had used certain medical facilities and what those type of facilities were, who the doctors were and giving the enquiring individual the name of the doctor so that he could possibly obtain information concerning the treatment, if any, that the individual subscriber may have received. This would be clearly prejudicial to that individual.

In a like fashion I think it is equally as clear why the legislature passed section 26 of the Family Law Reform Act. In order to enforce maintenance orders from either the Supreme Court or through the Provincial Court (Family Division) an address for the respondent must be obtained so that he can be served with the necessary papers indicating to him that he was in arrears and that he was being summonsed before the Court to show cause why he would not be dealt with by that Court for non-payment under an order. In so many instances it has in the past been a fairly simple procedure for a

debtor to avoid his creditors by moving frequently and not advising the creditor of his new address. Although there are agencies available to a creditor, or in this instance an applicant, to trace a respondent, it is time consuming and expensive to employ such individuals for that purpose. The applicants for enforcement are generally those persons who have not been receiving any monies and who are in necessitive circumstances by reason of that and cannot afford the costs of tracing the respondent. The Act wanted to provide as orderly a method as possible and as inexpensive a method as possible of locating the respondent and having that individual come before the Court as quickly as it could be managed.

In my opinion, in no way does section 26 of the Family Law Reform Act go against the obvious intention of section 44 of the Health Insurance Act. It would provide the enforcing Court under a maintenance order of the address of the respondent, debtor, but would not provide any information as to whether that individual, in fact, was insured through the Ontario Health Insurance Plan, whether that individual is providing coverage under that Plan for any other individual, whether that individual had used any services of a doctor or other medical facility nor would the information provided indicate who the doctor was, when he may have been seen, or provide any further details about that individual other than the last address that the Plan had of the individual. I think it is most important to stress this fact--that no information could be provided that would go against the intention of section 44 of the Health Insurance Act. It is my opinion that both Acts can stand side by side and both are within the legislative competence of the Ontario Government and that one section does not in any way offend the relevant section of the other Act. I am quite convinced that had the Family Law Reform Act, 1978 been in existence at the time of the passing of the Health Insurance Act, there would have been



an exception clearly placed in section 44 which would indicate that where an application had been brought under the Act for purposes of enforcement of an existing order, or for a support and/or custody application, that the Ministry would have been given permission to release the last known address of the respondent.

The distinction between enrolment information and health information is of fundamental importance. Enrolment information, as I have said, consists of the name of the subscriber or his dependants, the name and address of an employer or the home address. Health information, on the other hand, includes the name and address of the hospital, health facility, or person supplying insured services, the date upon which the services were performed, amounts paid, to whom the amounts were paid, diagnostic information, and fee schedule information. Health information is collected by OHIP for insurance purposes and is highly sensitive. No one, including the police, who is not involved in the administration of the Plan ought to be permitted ready and easy access to this information. OHIP must have a continuing obligation to keep this information confidential, an obligation that must take precedence over the desire by the police for information. So far in this discussion I have not been concerned with information to be obtained by invoking the judicial process.

I have examined the circumstances in which OHIP information was sought by the police and have described some representative situations. I did not encounter one example of an emergent situation, that is, one in which the information from OHIP had to be obtained within critical time limits so that, if a warrant were required in order to be entitled to the information, the resulting delay in obtaining the OHIP information would be harmful to a person or to society at large.

The police assert that section 44 of The Health Insurance Act, 1972, in its present form, prohibits the obtaining of sufficient information upon which a police officer might form a belief, on reasonable and probable grounds, that OHIP has in its custody relevant health information, with the result that they are unable to obtain a search warrant. One of the examples given above was that of a police officer's attempt to determine the names of physicians whom a deceased had seen six months before his death. The police officer did not know whether OHIP had any relevant information. I believe that an OHIP official in response to a question of that kind should not be prevented from telling the police that, "Yes, our records indicate that

this individual has seen certain physicians within this period." The OHIP official ought not be permitted to provide the names of those physicians or any other health information. However, having received this information, the police officer would have the reasonable and probable grounds that form the basis for obtaining a search warrant, if one were justified in the circumstances, which would permit the disclosure of the real information sought. In this situation, however, resort to a judicial officer would be involved. Particularized health information would only be disclosed after a decision was made that a search warrant ought to issue. A safeguard would be brought into play to ensure that the police were not attempting to obtain health information from OHIP for any improper purpose.

*Recommendations:*

15. (1) *That the district manager of OHIP or a person designated by him or her in writing at a district or satellite office, and only such a person, be permitted to disclose enrolment information to the police.*
- (2) *That the person so designated must ensure that the person seeking the enrolment information is, in fact, a police officer by requiring the police officer to attend in person or by the use of a call-back system.*
- (3) *That a log be maintained at every district and satellite office to record the date of the request, the name of the person seeking the information, his or her police force, his or her badge number, the subscriber or person about whom information was requested, and why the information was sought and given.*
16. *That OHIP be required to report yearly to the Minister of Health particulars of the number of requests received from the police, in general terms, the circumstances under which information was sought and the number of occasions on which enrolment information was given. The Minister of Health should make full*

disclosure of this OHIP report to the public.

17. That no employee of OHIP be permitted to release health information to any police force without a search warrant. The district manager of OHIP or a person designated by him or her in writing at a district or satellite office should, however, be permitted to answer, yes or no, to the question of any police officer whether OHIP has specific health information about a named person.
18. (1) That the director of the Insurance Claims Branch of OHIP or a person designated by him or her in writing be permitted to disclose, in writing, enrolment information to the Department of Employment and Immigration, in response to a written request setting out the purpose for which the enrolment information is required.  
  
(2) That OHIP keep a copy of every written request and reply in a central location.
19. That OHIP be required to report yearly to the Minister of Health particulars of the number of requests received from the Department of Employment and Immigration, the purpose for which the enrolment information was required, the number of requests and the number of occasions on which enrolment information was given. The Minister of Health should make this OHIP report public.

In my opinion, these recommendations fairly balance the obligation of confidentiality which OHIP has to the subscriber and his or her dependants, and the public need for disclosure of health information in situations in which that information is important to current police investigations.

A discussion of the relationship between the police and OHIP would not be complete without a reference to Lawrence Martin's story in The Globe and Mail of November 14, 1977, in

which it was alleged that the police had had access to OHIP records. OHIP is, of course, the responsibility of the Ministry of Health. The Minister of Health, the Honourable Dennis Timbrell, and the Deputy Minister at the time, W. Alan Backley, attempted to determine whether these allegations were true. To do so they held several meetings in the period November 14, 1977, to November 30, 1977. Attendance at the meetings varied, but on most occasions those present were Mr. Timbrell, Mr. Backley, Gordon Fetherston, the General Manager of OHIP, David S. Buchanan, and John R. Harnett. Mr. Harnett and Mr. Buchanan, it will be recalled, reported directly to Mr. Fetherston who, in turn reported to an assistant deputy minister. Obviously, Mr. Timbrell and Mr. Backley were concerned to know the real extent to which information had been released from OHIP without the authorization of the persons to whom the information related. That is what Mr. Timbrell instructed Mr. Fetherston to find out. According to Mr. Backley, Mr. Fetherston was specifically directed "to ascertain the number of contacts both from the point of view of providing patient names and addresses, and whether or not there had been any instances of medical information being provided." Mr. Fetherston disagreed with Mr. Backley's evidence in this respect. He took a narrower view and testified that the Minister wanted to know only the number of times the police had been given information by OHIP. Without hesitation, I accept Mr. Backley's evidence on this issue in preference to that of Mr. Fetherston both because Mr. Backley was a more satisfactory witness and because it is entirely consistent with common sense that the Minister would be interested in the broad view. I add that I am satisfied that, before the publication of Mr. Martin's story in The Globe and Mail, neither Mr. Timbrell nor Mr. Backley nor their predecessors had any idea that OHIP had been disclosing information to the police.

Mr. Fetherston, in due course, advised the Minister that the police had been provided with enrolment information only on 24 to 30 occasions per year. Mr. Timbrell relied upon the accuracy of this information. As I have said, he wanted to determine the extent to which there had been unauthorized disclosures of information from OHIP. He was led to believe that information was released only to the police in breach of section 44 of The Health Insurance Act, 1972. Even if Mr. Fetherston sincerely believed that the Minister was interested merely in learning the frequency with which the police had been given information from OHIP, he and Mr. Harnett discharged their responsibility to their Minister unsatisfactorily by failing to advise him of OHIP's relation with the Immigration Department and of the 60 to 70 monthly requests and responses that Mr. Harnett's administrative assistant personally handled from

that Department. Moreover, the estimate given to the Minister was inaccurate. The most cursory canvass of employees at the various district offices would have disclosed that contacts with the police were accepted as routine and frequent. The evidence at our hearings disclosed that the number of contacts was at least 80 per year.

The fact that the Minister was given an inaccurate estimate and that no one voluntarily advised him of OHIP's relationship with the Immigration Department is disturbing but, in my experience, not atypical. It is also significant that no one at OHIP volunteered the information about the relationship between the Immigration Department and OHIP to us. It was only as a result of our independent investigation that this relationship and its extent were discovered. The Minister was not informed of the relationship until March 2nd, 1978, when he was given this information by Mr. Strosberg. The failure or refusal to volunteer information known to be relevant to my inquiry also characterized my relationship with senior officials of OHIP.

I have concluded that Messrs. Fetherston, Harnett and Buchanan did not give confidentiality a high priority. They were primarily concerned with the efficient processing of claims. It is significant to me that their inquiry in response to their Minister's request to determine the extent of the disclosure of information from OHIP was carried out by a hurried and entirely unsatisfactory telephone canvass of the district directors. Surely there should have been an effort to follow up the oral inquiries with a more careful and detailed questionnaire, given the importance that the issue had assumed. No such follow up was ever carried out.

Perhaps Mr. Buchanan best reflects the attitude of the senior OHIP officials. Despite the fact that several district directors had denied being contacted by him in November, 1977, despite the fact that he had not kept any notes of these contacts, and despite the fact that he had not been present to hear the sworn testimony of OHIP employees at our hearings, he steadfastly maintained, under oath, that the estimates given to the Minister of 24 to 30 contacts per year had been accurate.

Mr. Buchanan's relationship with Bruce Gerald Russell Adams, a conscientious Ministry of Health employee at the Oshawa District office, is also illustrative of Mr. Buchanan's attitude toward confidentiality. Mr. Adams took a keen interest in the issue of confidentiality. He was also interested in the issues of record management and recycling of paper. He believed that proper disposal of paper, according to definite destruction



schedules went hand and hand with, and promoted, confidentiality. Mr. Buchanan recognized Mr. Adams' interest and expertise in this area for, in the fall of 1976, Mr. Buchanan instructed Mr. Adams to prepare a report on the issue of confidentiality as it related to the company responsible for the Ministry of Health's recycling. Commencing in December, 1976, Mr. Adams showered Mr. Buchanan with requests for meetings. He was unsuccessful in arranging any. Mr. Adams contacted Mr. Buchanan about 15 times a year complaining about OHIP's failure to enforce policies of confidentiality. In the spring of 1977, approximately 275 IBM claim cards were found in a parking lot and Mr. Adams was asked to determine the source of these documents. Mr. Adams dutifully provided his opinion by written memorandum dated July 11, 1977, addressed to Mr. Buchanan. After giving his opinion as to the source of these cards, his memorandum continued as follows:

Confidentiality within OHIP and the Provincial Government is ludicrous, in that, the volume of paper created is only maintained during the initial or activity period. Following these periods, the documents are handled by lesser staff who do not know, are not instructed, or are careless in handling this material at a later date. Some examples are:

- (a) Medical claims cards are processed at a rate of 4 to 5 million a month and held for a period of three months in overcrowded files or boxes. When it is time to move these documents due to the volume, internal staff boxes or stuffs the cards into bags; should a few cards be missed or fall on the floor, they are ignored or shoved in wastebaskets. When I complained during my visits to the District Offices, the general attitude was "So what! We have no time to be that careful."
- (b) Documents considered confidential by some parts of OHIP are thrown in bulk bins adjacent to operating areas of Overlea Boulevard. These papers and documents can be blown out into the roadway or streets surrounding the area and nobody would pick them up or take time to bring to the attention of those

responsible, that these factors are occurring. This also applies to the Queen's Park area.

- (c) In addition, it is a known fact that employees of the bulk firms are extracting paper and documents from these bins and are selling the contents to various recycling firms, which is causing a continuing loss of confidentiality plus a loss of remuneration to the Treasury of Ontario (names can be given if required).

Records Management, through its retention of documents has established times to eliminate storage or hoarding of useless documents, thereby saving space in areas, but the destruction of documents is left to the individual areas to decide the manner of destroying materials, e.g. confidential, non-confidential, by burning, shredding, garbage or recycling.

The points raised are valid, and at any time you wish to satisfy yourself, I would be able to prove these statements at any location you select.

My suggestion would be to send out an instructional letter to all district offices explaining these problems, then policing the districts to ensure that proper handling methods are carried out to protect the confidentiality of our Practitioners and Subscribers. This would cause the Directors of each district office to complain justifiably, of manpower and space.

If you are really concerned about confidentiality and recycling, which I doubt, then more creative action will have to be taken to correct the situation as it now stands.

Several times, I have phoned your office in regards these problems, but have yet to receive an answer. [emphasis added]

Mr. Adams received no reply from Mr. Buchanan to this memorandum. His numerous telephone calls made to Mr. Buchanan's office were ignored. As he put it, his "pleas were falling on deaf ears." Mr. Adams' opinion, an opinion I find accurate, was that confidentiality was a low priority with Mr. Buchanan. Mr. Adams should be highly commended for recognizing the importance of confidentiality in a health-care system. In many respects his was a solitary voice.

## Police, Physicians and Hospitals

A physician has both an ethical and a legal obligation to keep his or her patients' health information confidential. The legal obligation is found in the following provision in Regulation 577/75 made under the authority of The Health Disciplines Act, 1974, S.O. 1974, chapter 47:

26. For the purpose of Part III of the Act,  
"professional misconduct" means,

. . . . .

21. giving information concerning a patient's condition or any professional services performed for a patient to any person other than the patient without the consent of the patient unless required to do so by law;

It will be observed that the physician's obligation of confidentiality is expressed in absolute terms and permits disclosure of information, without patient consent, only where it is required by law. In my opinion every employee of a physician has an obligation to his or her employer to respect the confidentiality of any information he or she has about that physician's patients.

A public hospital's obligation of confidentiality is found in the following provisions of The Public Hospitals Act, R.S.O. 1970, chapter 378, and Regulation 729 made thereunder:

### THE PUBLIC HOSPITALS ACT

11. The medical record compiled in a hospital for a patient or an out-patient is the property of the hospital and shall be kept in the custody of the administrator.

36. Every person who contravenes or is a party to the contravention, directly or indirectly, of any provision of this Act or the regulations is guilty of an offence and on summary conviction is liable to a fine of not less than \$25 and not more than \$500.

R.R.O. 1970, Regulation 729.

48. (1) Subject to subsections 2, 3, 4 and 5, a board shall not permit any person to remove, inspect or receive information from a medical record.

(2) Subsection 1 does not apply to,

(a) a person with a process,

(i) issued in Ontario out of a court of record or any other court, and

(ii) ordering the removing of, the inspecting of or the receiving of information from a medical record; or

(b) an inspector.

(3) Notwithstanding subsection 1, a coroner or a legally qualified medical practitioner, magistrate or police officer so authorized in writing and directed by a coroner, may inspect and receive information from medical records and may reproduce and retain copies therefrom for the purposes of an inquest or to determine whether an inquest is necessary, where the coroner has,

(a) issued his warrant to take possession of the body;

(b) issued his warrant for an inquest; or

(c) attended at the hospital to view the body and make an investigation in accordance with The Coroners Act.

. . . . .

(5) A board may permit,

- (a) the attending physician;
- (b) the administrator of another hospital who makes a written request to the administrator;
- (c) a person who presents a written request signed by,
  - (i) the patient,
  - (ii) where the record is of a former patient, deceased, his personal representative; or
  - (iii) the parent or guardian of an unmarried patient under eighteen years of age;
- (d) a member of the medical staff but only for,
  - (i) teaching purposes, or
  - (ii) scientific research that has been approved by the medical-staff advisory committee;
- (e) a person with a written direction from the Deputy Minister of Veterans Affairs (Canada) or some person designated by him, where the patient is a member or ex-member of Her Majesty's military, naval or air force of Canada; or
- (f) the Director of the Research and Planning Branch or the Department or his authorized representative approved by the Commission or an officer or



employee of the Commission who  
is designated by the Chairman,

to inspect and receive information from a  
medical record and to be given copies there-  
from.

(6) Any information received under  
clause f of subsection 5 shall not be used  
or disclosed to any person for any purpose  
other than the purposes of compiling  
statistics and carrying out medical and  
epidemiological research for or approved by  
the Department and the Commission.

. . . . .

Hospital employees have an obligation to maintain confidential-  
tiality in all circumstances except those in which the hospital  
is entitled to disclose information about patients.

On December 8, 1977, a story by reporters Lawrence Martin  
and Paul Palango appeared in The Globe and Mail. The headline  
read, "Police Use Intimidation To Get Medical Files, Hospital  
Workers Say". The story, which, according to Mr. Palango, was  
written within about three hours before press time, was the  
result of a telephone canvass of various hospital employees in  
the Metropolitan Toronto area. The story quoted Diane Davis,  
who, at the time of her testimony at our hearings, had become  
Mrs. Diane Manual, as saying that "most of the police problems  
involved the OPP." Mrs. Manual denied that she had made such a  
statement and I accept her evidence. However, one of the chief  
points made in the story was certainly true and was confirmed by  
the evidence of several hospital administrators and medical re-  
cord administrators or librarians. On various occasions, police  
officers have attempted to obtain health information from  
hospitals throughout the province, without patient authoriza-  
tion. Sometimes, when they were refused such information, some  
officers became abusive and, although rarely, threatened to  
charge the unco-operative hospital employee with obstructing  
justice. A charge of that sort, of course, in a situation in  
which there was neither patient consent nor a search warrant,  
would be groundless. In any event, no hospital employee was  
able to give the name of any police officer who had made a  
threat of that sort and the evidence as to time and the identity  
of the police forces involved was imprecise. It is clear, how-  
ever, that it was inaccurate to say, as The Globe and Mail story  
went on to say, that "most of the police problems involved the  
OPP." The fact is that the chief point made was applicable to

almost all police forces across Ontario, although on isolated occasions only. That this has been a general phenomenon may be illustrated by the attitude revealed in the brief of the Ontario Association of Chiefs of Police. It referred to instructions issued by the Middlesex Elgin Hospital to its staff in December, 1977, which, properly, recited that it was not the hospital staff's responsibility to report to the police such matters as gunshot wounds, stab wounds, suspected illegal abortions, and drug overdoses. In connection with these instructions, the brief said,

In my opinion the instructions that have been given with respect to serious crimes almost verges upon obstruction of justice.

Mrs. Manual estimated that on three or four occasions during her four-and-one-half year tenure as medical record administrator at the Scarborough General Hospital, police officers had visited her, requested confidential health information without patient authorization or warrant, and upon her refusal, threatened her with arrest. Mrs. Manual did not know the names of these officers or the force or forces involved except that, on one occasion, it was a Metro Police officer. In her testimony, Mrs. Manual emphasized that, despite the threat, she was "not intimidated by it." In this respect, Mrs. Manual was typical of almost all the medical record administrators and hospital administrators who appeared at our hearings. They were not intimidated by these infrequent and isolated threats. Faithfulness to the principle of confidentiality on the part of these hospital employees in these circumstances was clearly proved by the evidence. It is largely because I am certain that medical record administrators, supported by their hospital administrators, can be relied on to act in accordance with their expressed commitment to confidentiality that I have confidence in the adequacy of the recommendations that follow.

During the course of our hearings, evidence was given of the occurrence of violations of the regulations by the disclosure of health information without patient approval. On the other hand, examples were also given of compliance with the prohibition in the regulations in circumstances in which physicians and hospital employees might well have been morally justified in making disclosure despite the law. It will be helpful to describe seven general situations, with examples of each, in which hospital employees and physicians have disclosed health information without patient authorization despite the language of the legislation. There will be seen throughout the eternal conflict between the obligation to, and the rights of, patients and the public's need for, or interest in, protection.

In the first situation, a request for information is made by the police to a physician concerning the mental or physical condition of a patient in connection with a crime in progress in order to know how best to approach a violent person in a way that would minimize danger. A helpful illustration was given at our London hearings by William B. Pogue, the executive director of the Woodstock General Hospital. In an incident that occurred a few years ago, the police in another jurisdiction in which an aircraft hijacking was taking place contacted the Woodstock police who in turn communicated with the hospital. The hijacker had been treated at the hospital and information was given to the police from his medical record without his consent. Assisted by that information, the police were able to bring the hijacking to a satisfactory conclusion. Although disclosure of information from the medical record in these circumstances is not permitted under the provisions of The Public Hospitals Act, or Regulation 729, it is probable that few reasonable persons would condemn the hospital's conduct. In another example, a treating psychiatrist in Metropolitan Toronto was consulted about a patient who was holding several persons hostage. The psychiatrist gave the police information about his patient's mental health which helped them to deal with the patient and permitted them to end the hostage-taking incident peacefully. Again, the disclosure was prohibited, but most persons would excuse the psychiatrist's breach of the statutory duty in the circumstances.

The second situation does not involve a request by the police or any public official. The ethical dilemma arises when the hospital employee or physician must decide whether he or she ought to act purely on the basis of his or her own assessment and information about his or her patient that has not, as yet, been shared with, or become known to, anyone else. This situation may occur when, for example, a physician becomes aware of the commission of an offence either because of the patient's physical condition, or an admission made by him or her, perhaps in psycho-therapy. Similarly, a physician may become aware of a threat of violence against another or others made by his or her patient. An example of this situation is found in the brief submitted by the London Police Force.

A recent case in London can be directly related to the dilemma a psychiatrist must face in the physician/patient relationship.

Russell Johnson and his wife were interviewed by a psychiatrist in 1969 in the course of which he informed the psychiatrist that he had broken into an apartment and

sexually attacked a woman. He was given a voluntary admission to the Psychiatric Hospital, remained for a short period but subsequently signed himself out.

During this time, the police were actively investigating this crime but were not contacted by the psychiatrist to verify whether in fact this crime had been reported or that the facts as given by Johnson were in fact true. The police continued to investigate this crime with no concrete leads. A series of murders and sexual assaults, extending from 1969 to 1977 took place in which seven (7) females met their death and sexual attacks took place on ten (10) other women. Johnson was subsequently arrested in July, 1977 and charged with the murder of three (3) of these females. He was found not guilty by reason of insanity and is presently in Penetanguishene.

Had the original information on Johnson been made available to the police on the confidential basis, the other crimes may not have been committed. A discreet investigation would have been carried out which in all probability would have resulted in Johnson's arrest.

The third situation, again, does not involve a request by the police or a public official and is a slight variation of the second. A physician or hospital employee learns that his or her patient has been involved in a completed crime which the police do not know about. Many examples of this type of situation were given throughout our hearings. Section 251(2) of the Criminal Code, R.S.C. 1970, chapter C-34, makes it an offence for a female person who is pregnant to use any means, or to permit any means to be used on her, to procure a miscarriage. In the first example, a young girl presents herself at the emergency department of a public hospital showing signs of, and admitting to, an illegal abortion. Should the hospital staff or attending physician report this to the police? Should they be required to report this to the police? In at least one case a hospital did in fact report the matter to the police against the wishes of the patient.

Another example of the third situation is that of a patient who presents himself or herself at a hospital with a bullet



wound or a stab wound. The stab wound is the result of a domestic fight between husband and wife while both were intoxicated. Each forgives the other and neither desires to involve the authorities. In these not uncommon circumstances, is it necessary that the police be involved? Some hospital administrators admitted that it was their hospitals' policy to report bullet and stab wounds to the police even though to do so is contrary to the provisions of Regulation 729. A further example is that of a young person who presents himself or herself to a hospital suffering from the effects of an hallucinogenic drug such as LSD. Should the hospital notify the police that the patient possessed and consumed the drug?

These examples raise the question whether hospitals and physicians should be bound to report to the police the names of patients whose conditions suggest involvement in illegal activities. If mandatory reporting were introduced there would be no discretion to refrain from reporting, even if the hospital employee or physician reasonably believed there was no risk of future harm. I shall have more to say later about the issue of mandatory reporting.

I turn to the fourth situation. In Ontario, the OPP have primary responsibility for the protection of the Lieutenant-Governor, the Premier, members of the Ontario Cabinet and others. The RCMP have the primary responsibility in the following cases:

1. the provision of similar preventive protection for the Royal Family, the Governor General of Canada and his or her family, the Prime Minister and his or her family, Ministers of the Federal Crown, Supreme Court Judges, and other prominent Canadians;
2. the provision of preventive protection for visiting dignitaries and Heads of State, pursuant to Canada's obligation under the United Nations Convention for the Protection of Internationally Protected Persons, preventive steps to forestall the commission of any of the crimes specified in section 6(1.2) of the Criminal Code, as amended by S.C. 1974-75-76, chapter 93, section 3(1), against "internationally protected persons" (as defined in section 2 of the Criminal Code, as amended by S.C. 1974-75-76, chapter 93, section 2(1)) or their premises; and
3. the provision of preventive protection for foreign diplomats and embassies and consulates in Canada pursuant to Canada's obligations under the Vienna Convention.



In police circles, these responsibilities are known as VIP protection. All the police forces, national, provincial and municipal, give each other full co-operation no matter which force has the primary responsibility. This fourth situation exists when the RCMP or the OPP are concerned that the patient inquired about may pose a threat to a "VIP". The inquiring officer is usually attempting to elicit an opinion as to whether or not the patient is likely to do harm to the person being protected or is likely to carry out a threat he or she has made. In most cases the precise diagnosis is immaterial.

The RCMP admitted that they had made at least 135 inquiries of physicians, hospitals or hospital employees during the execution of their VIP responsibilities. They informed me of the names of the officers who made the inquiries, the dates of the inquiries and, in general terms, the reason for the inquiries and the nature of the information given in reply. They have, however, refused to identify the physicians and hospital employees who disclosed this information. The Court of Appeal, in Re Inquiry into the Confidentiality of Health Records in Ontario (1979), 24 O.R. (2d) 545, 98 D.L.R. (3d) 704, 47 C.C.C. (2d) 465, in response to questions put by me in a case originally stated in the Divisional Court, held that the RCMP had no right to withhold from this inquiry the names of physicians and hospital employees who, without patient consent, gave them health information about their patients, contrary to the relevant provision of Regulation 577/75 under The Health Disciplines Act, 1974 and Regulation 729 under The Public Hospitals Act. An appeal from the judgment of the Court of Appeal is now pending in the Supreme Court of Canada. I have concluded that to postpone the conclusion of this report and the making of recommendations, in the expectation that this question can eventually be dealt with, would delay the report too long. This aspect of the inquiry therefore cannot be completed until the decision of the Supreme Court of Canada has been rendered and then, of course, only if the appeal has been dismissed.

Our own investigation established that nine psychiatrists throughout the Province have provided health information about their patients to the RCMP, OPP and the Metro Police forces. It would, I believe, serve no good purpose to disclose the names of these psychiatrists. To do so would be contrary to the interests of the patients who might be identified by the disclosure of the circumstances, of the psychiatrists, who might well be exposed to danger at the hands of some of these patients or, for that matter, of other patients of these psychiatrists, who might incorrectly draw the conclusion that their psychiatrists have given information about them to police officers.

Through their counsel, these nine psychiatrists made a statement which, I am entirely satisfied, accurately reflects their beliefs and explains why they disclosed information to the police without their patients' authorization. The statement was in the following terms:

1. The physicians in question were contacted on one or more occasions by various police officers throughout the Province of Ontario.
2. The police inquiries concerned the physicians' patients who:
  - (a) had allegedly made threats against public figures; or
  - (b) were suspected of crimes of violence.
3. The police officers wished to determine whether the patients were capable of carrying out their threats or capable of committing crimes of violence.
4. The physicians, from time to time, expressed opinions in response to inquiries without the patient's authorization and knowledge.
5. The physicians acknowledged that they had an obligation to keep information confidential and not to reveal it without the patient's consent.
6. The physicians, nevertheless, believed that they had an overriding public duty to answer inquiries of the kind made by the various police officers, notwithstanding their obligation of confidentiality to their patients.

It will be useful to set out seven examples given by the RCMP and which our independent investigation revealed are similar to the cases in which the nine psychiatrists disclosed health information without patient consent. None of these examples is a case in which any of the nine psychiatrists was involved. The examples are as follows:

- (a) Corporal P. Fatijwski of the RCMP was investigating an individual who was forceably removed from the Prime Minister's residence. The corporal contacted a psychiatrist who, without the patient's authorization, told him that the patient had been admitted to an Ontario institution on four occasions between 1968 and 1972, was a paranoid schizophrenic, suspicious of everyone and everything, had a persecution complex, which had led to two attempts at suicide, but was dangerous only to himself and that physical threats made against anyone else were unlikely to be acted upon.
- (b) In late 1974, Corporal Stewart was investigating a person who had threatened to kill a Canadian ambassador. The corporal interviewed a physician in Ontario, who, without his patient's authorization, told him that the patient was excitable, capable of acts of aggression, potentially dangerous to persons in authority, had threatened to "get even" with his physicians who had testified during a previous trial and if provoked, would do almost anything.
- (c) On January 16, 1973, Corporal Black of the RCMP investigated a person who had threatened to kill a son of a member of Parliament. The corporal contacted a physician who, without his patient's authorization, revealed that the patient was a paranoid schizophrenic and was potentially dangerous.
- (d) Sergeant D. Delaney, of the RCMP, while investigating a person who had instigated a bomb hoax, contacted an unknown hospital employee who revealed that the patient had been committed to a specified institution, on a specified date in 1964 as a result of a court order and remained there for one year, provided the patient's physical description and particulars of the next of kin. This unknown hospital employee also said that the patient had been committed as a result of a criminal charge, had been diagnosed as mentally disturbed, having a pathological personality, and being a sex pervert. He characterized the patient as a sex pervert, and loner capable of becoming easily depressed, sometimes hostile, suffering from the occasional epileptic seizure but with an improved condition at the time of the disclosure.
- (e) Constable Washburn, in 1976, was investigating an individual who had threatened to kill the Prime Minister. He contacted the individual's physician who stated that the patient was not a threat to anyone. The physician confirmed that the subject was schizophrenic and that it was

during a depression that he had threatened to kill the Prime Minister.

- (f) In 1970, Sergeant Chad and Corporal Swainson of the RCMP contacted a psychiatrist in an Ontario institution who revealed that a patient, who had threatened the Prime Minister, had a manic depressive syndrome and had been in a hypermanic state. The psychiatrist said that the patient became psychotic when called a communist, had a tendency to lose sight of reality but was more a nuisance than dangerous.
- (g) Sergeant Man and Constable Nicholson of the RCMP, were investigating a person who persistently followed the Prime Minister in a taxi. They contacted a physician in 1973 who told them that his patient had been admitted to a general hospital in mid 1969 complaining of heart pains. At the time of the admission, it became clear that the patient was mentally disturbed with the result that he was admitted to the psychiatric unit where he was treated by the psychiatrist. The psychiatrist, in his report to this physician, diagnosed the subject as a "definitely psychotic young man". The physician explained that the patient thought that he was evaporated by God, that he had received his mother's heart and that his mother had received his heart. The diagnosis was "schizo-affective psychosis". It was this physician's opinion that the patient was capable of murder, suicide or assassination, that he was totally unpredictable, could be triggered by any event, a wrong word or nothing at all and there was no effective way of treating the patient whose actions were always at the extreme of depressed and quiet to violent and aggressive. He also stated that the patient became physically violent when told what to do and that any threats made by him should be taken seriously. In the fall of 1974, Sergeant Man contacted a different physician who was of the view that the patient was very intelligent, with sharp insights, well meaning, verbal as opposed to physical and had control of his faculties, did not require medication, was not drug oriented, was not violent and incapable of physical harm. This second physician's conclusion was that his patient was an unconventional thinker who would, however, not hesitate to cause embarrassment and was quite capable of doing so.

In the fifth situation a person applies for a firearm acquisition certificate, more commonly known as a gun permit. The Thunder Bay Police Department contacted the Lakehead Psychiatric Hospital on approximately 25 occasions to determine whether an applicant for a gun permit had ever been a patient

there. The hospital answered the inquiries. If the hospital's answer was negative, further inquiry was unnecessary. If the hospital's answer was in the affirmative, as it was once, the police officer attempted to obtain further health information. In my view, this type of inquiry ought to be prohibited. The Criminal Code, S.C. 1976-77, chapter 53, section 3, proclaimed in force January 1, 1979, sets out the criteria relevant to the determination of whether a gun permit ought to be issued. The relevant provisions are as follows:

104.(1) Where a firearms officer to whom an application for a firearms acquisition certificate is made, after considering the information contained in the application, any further information that is submitted to him pursuant to a requirement made under subsection (8) and such other information as may reasonably be regarded as relevant to the application, does not have notice of any matter that may render it desirable in the interests of the safety of the applicant or any other person that the applicant should not acquire a firearm, he shall, subject to subsection (2) and on receipt by him of the appropriate fee, if any, issue a firearms acquisition certificate to the applicant.

. . . . .

(3) A firearms officer shall be deemed to have notice of a matter that may render it desirable in the interests of the safety of an applicant for a firearms acquisition certificate or of any other person that the applicant should not acquire a firearm and a magistrate, on a reference pursuant to subsection (6), is entitled to confirm the opinion of a firearms officer that it is not desirable in the interests of the safety of such applicant or of any other person that such applicant should acquire a firearm, where it is made to appear to him that the applicant

. . . . .

(b) within five years, immediately preceding the date of his application, has been treated for a mental



disorder, whether in a hospital, mental institute or psychiatric clinic or otherwise and whether or not he was, during that period, confined to such a hospital, institute or clinic, where the disorder for which he was so treated was associated with violence or threatened or attempted violence on the part of the applicant against himself or any other person; or

- (c) has a history of behaviour occurring within five years immediately preceding the date of his application, that included violence or threatened or attempted violence on the part of the applicant against himself or any other person.

. . . . .

(7) An application for a firearms acquisition certificate shall be in a form prescribed by the Commissioner and shall be made to a firearms officer.

(8) A firearms officer to whom an application for a firearms acquisition certificate is made may require the applicant to submit such further information in addition to that included in the application as may reasonably be regarded as relevant for the purpose of determining whether there is any matter that might render it dangerous for the safety of the applicant or of any other person if the applicant acquired a firearm.

It would be a simple matter to incorporate in an application for a permit an authorization to release health information. Given the ease with which it could be obtained, in the absence of an authorization no psychiatric facility or psychiatrist ought to release health information for this purpose. It is not without significance that despite the fact that there were many examples of co-operation between hospital facilities and physicians, on the one hand, and the police on the other, no police force other than the Thunder Bay Police Department adopted the practice described. It is equally

significant that, although we received briefs from several police forces, none of them suggested that it was necessary to obtain health information without patient authorization for the purpose of evaluating applications for gun permits.

The sixth situation exists when the police are aware that a crime has been committed and are seeking the perpetrator. The leads which the police have relate to health information. The hospital or physician does not know that a crime has been committed but has health information about its, his or her patient which, if given to the police and considered along with the information that the police have, would result in the arrest of the patient as the perpetrator. The search warrant provisions of the Criminal Code are in the following language:

443.(1) A justice who is satisfied by information upon oath in Form 1, that there is reasonable ground to believe that there is in a building, receptacle or place

- (a) anything upon or in respect of which any offence against this Act has been or is suspected to have been committed,
- (b) anything that there is reasonable ground to believe will afford evidence with respect to the commission of an offence against this Act, or
- (c) anything that there is reasonable ground to believe is intended to be used for the purpose of committing any offence against the person for which a person may be arrested without warrant,

may at any time issue a warrant under his hand authorizing a person named therein or a peace officer to search the building, receptacle or place for any such thing, and to seize and carry it before the justice who issued the warrant or some other justice for the same territorial division to be dealt with by him according to law.

. . . . .

It will be observed that, to be entitled to a search warrant, a police officer must have reasonable grounds for believing that the relevant evidence can be found in a given hospital or in the possession of a given physician. Moreover, search warrants authorize the seizure of things--in the present context, medical records; they cannot compel the disclosure of unrecorded information. A helpful illustration is a case that arose in Toronto. A man entered a shop and was noticed by a salesgirl. He left the shop without transacting any business. The next day he returned. He had a cast on his right arm that had not been there at the time of his first attendance. He raped and robbed the salesgirl. The Metro Police concluded that the cast has probably been applied in a Toronto hospital in the interval between the first attendance and the time of the rape and robbery. However, they did not know which hospital the suspect attended and were unable to obtain a search warrant. The police thereupon canvassed Toronto hospitals, armed with a description of the assailant from the salesgirl. An employee of a hospital, when questioned, remembered the patient who had had a cast applied within the relevant period and who matched the description. The employee gave the police the patient's name. The patient was confronted, confessed and was later convicted of rape and robbery. The apprehension and conviction would have been impossible without the aid of the hospital employee who supplied health information to the police in contravention of Regulation 729. In these circumstances a search warrant could not have been obtained and the hospital records alone would not have disclosed the proper person.

Another example occurred when the Metro Police discovered the body of a person who had been stabbed to death in a Toronto park. The deceased had a knife clutched in his right hand. Blood was found leading away from the corpse. It was a reasonable inference that the assailant had also been stabbed and was injured. The police immediately went to the nearest public hospital and, in the emergency department, asked whether any patient had presented himself or herself with stab wounds. A hospital employee informed the inquiring officer that, at that very moment, a physician was suturing a patient with a stab wound. The police arrested the patient and charged him with manslaughter. He was later convicted. The disclosure by the hospital employee was not permitted by Regulation 729.

A further example relates to thefts of motor vehicles. A motor vehicle is stolen and wrecked in circumstances which give rise to a reasonable inference that the operator was injured. The police canvass all hospitals in the area of the accident and request the names of all patients who have been treated in the emergency department for injuries consistent with a motor

vehicle collision. The police match the names of all patients obtained against the list of reported collisions and are able to eliminate patients whose collisions were reported. The remaining patients become suspects in the theft. The evidence is that motor vehicle thieves are frequently apprehended in this fashion.

Hospitals also share information with the police in motor accident cases. At one hospital in Metropolitan Toronto, before November, 1977, unaccompanied police officers were permitted to enter the area in which the emergency department records were kept and allowed to read these records to obtain whatever information they needed to complete police reports.

The final example to be given of the sixth situation relates to the offence of breaking and entering. Not infrequently the targets are jewellery stores. Assume that entry is obtained by breaking through a glass window or door. The police find a pool of blood which is consistent with a cut to the perpetrator from the glass. The police immediately canvass all hospitals in the area to determine whether any patients have presented themselves for treatment for glass cuts. In many cases hospital employees gave the police the names of patients with appropriate injuries whose circumstances were then investigated by the police with the result that arrests and convictions ensued.

The seventh situation deals with former patients who are dead or are believed to be dead at the time of the inquiry. Often the police are concerned with the cause of death but, in disfiguring disasters such as fires and aircraft crashes, the identification of a dead body may be necessary. In these circumstances the police often make inquiries of a physician or a dentist to determine whether or not an individual who the police suspect is the deceased person has ever been treated by the physician or dentist. If he or she had been so treated, the police want access to x-rays or dental records that would aid in identification. In almost all cases, the police receive co-operation from hospitals, physicians and dentists in this situation. In these circumstances the privacy of the patient is surely not entitled to high priority. It seems to me that there can be no real objection to the giving of information to the police by a hospital, physician or dentist about a patient for the purpose of attempting to identify a body.

#### *Recommendation:*

- 20. That hospitals, health-care facilities and individual health-care providers be permitted to disclose information to the*

*police about a patient who the police reasonably believe is dead, for the purposes of aiding in the identification of a body.*

The examples given in the situations described above illustrate that physicians, hospital employees and other health-care workers have not always discharged their obligation of confidentiality. In many of these situations the disclosures were morally proper despite the current state of the law. This experience demonstrates that the practice relating to the disclosure of patient information without authorization diverges from the law. This deviation in practice and the underlying moral justification for it persuade me that the law ought to be amended. Before doing so, however, consideration must be given to the conflicting principles and interests involved.

On the one hand, the primary concern of physicians, hospitals, their employees and other health-care providers must be the care of their patients. It is not an unreasonable assumption to make that persons in need of health care might, in some circumstances, be deterred from seeking it if they believed that physicians, hospital employees and other health-care providers were obliged to disclose confidential health information to the police in those circumstances. A free exchange of information between physicians and hospitals and the police should not be encouraged or permitted. Certainly physicians, hospital employees and other health-care workers ought not to be made part of the law enforcement machinery of the state. On the other hand, the protection of the confidentiality of health information should not continue to be expressed in absolute terms. If there exists a significant or probable risk of serious physical harm to a person or if a serious crime has been committed, there may, in some circumstances, be a public interest that outweighs an individual's privacy interest and justifies the disclosure by a hospital employee, physician or other health-care provider of health information to the police without patient authorization.

Legislation in many jurisdictions in the United States requires hospitals and physicians to report gunshot wounds and stab wounds to the police. In effect, mandatory reporting exempts health professionals from the duty of confidentiality in certain circumstances by requiring the reporting of information that would otherwise be confidential. It was urged upon me in briefs filed by the London Police Force, the Ontario Association of Chiefs of Police, the Ontario Association of Children's Aid Societies, the Ontario Provincial Police and the Metropolitan



Toronto Police that I should recommend such a system of mandatory reporting for Ontario.

I have not been persuaded that a mandatory system of reporting bullet wounds, stab wounds and serious crimes is desirable. To ensure compliance a mandatory reporting system requires the imposition of a penal sanction on a person obliged to report in the event of a failure to report. In the contest between the interests of privacy and the maintenance of such fundamental relationships as that of husband and wife, on the one hand, and the interests of law enforcement, on the other, it is not always the case that the latter interest should have priority over the former. Not every injury inflicted by, say, a wife on her husband in the course of a violent matrimonial dispute, needs to be made a police matter through the instrumentality of the physician who treats the wounded husband. Mandatory reporting would make it a police matter without regard for the physician's judgment.

I have also been asked to recommend that physicians be required to report to the police all injuries that are consistent with the commission of a crime. I cannot do so. A requirement of that kind would make physicians statutory informers. The concept of confidentiality of health information would be seriously undermined and members of the medical profession would become part of the law-enforcement machinery of the Province. It was submitted that mandatory reporting would make police work and law enforcement more efficient. About that I have no doubt. Absolute crime control has not been and cannot be the goal of a society that would remain free. Because of the value of the other interests which we value, the lot of the policeman may always have to be not a happy one. As a society, we accept the need to balance the preservation of privacy and freedom with police efficiency. That is why search warrants are required and why the police must have reasonable and probable cause for obtaining them before a subject's privacy may be invaded. On the other hand, to prohibit physicians and hospitals from giving information to the police, no matter what the circumstances may be, seems to me to be equally objectionable.

#### *Recommendation:*

- 21. That no legislation be enacted that would require hospitals or health-care facilities, the employees of hospitals or health-care facilities, physicians or other health-care workers to report to the police gunshot wounds, stab wounds or any other injuries indicating the*

*commission of a crime or of a statement  
by a patient of any intention to commit  
a crime.*

The situations described above, and the examples of them given, afford ample justification for amending the legislation governing confidentiality to accommodate the demonstrated needs of society. The absolute requirement of confidentiality without patient authorization is unworkable. The existence of discretion in hospitals and physicians to disclose health information without authorization in some circumstances should be permitted. It is significant that the Canadian Civil Liberties Association itself, in its written brief, supported this position:

Subject to the adoption of effective safeguards to minimize the risk of abuse, health care workers might be relieved of the obligation to conceal information in those situations where they reasonably believe there is a significant risk of serious bodily injury. In other words, where such circumstances apply, health care workers might be allowed, but not compelled, to disclose sufficient data to avert the anticipated harm. Thus, even in the absence of a warrant, a psychiatrist might be able to use whatever he or she knows about a patient to assist the police in the event that such patient were involved in a hijacking or hostage taking incident. Conceivably, psychiatrists could even alert the police in advance of whatever such plots their patients may have confided to them.

In this part of the report, I have considered the issue only as it relates to hospitals and physicians, but the first recommendation below is equally applicable to other health-care providers. Further discussion of this issue may be found in the section of the report dealing with individual health-care providers.

#### *Recommendations:*

22. *That the relevant regulations under The Health Disciplines Act, 1974 be amended to provide that, where a health-care provider whose profession falls within The Health Disciplines Act, 1974 and who is not working in a health-care facility*

or under the direction of a physician has reasonable cause to believe that a patient is in such mental or emotional condition as to be dangerous to himself or the person of another or others and that disclosure of information about the patient is necessary to prevent the threatened danger, the health-care provider may disclose such information to the police or others without the consent of the patient. Disclosure made under that reasonable belief shall not amount to professional misconduct.

23. That legislation be enacted to provide that, when a senior official of a hospital or health-care facility has reasonable cause to believe that a patient is in such mental or emotional condition as to be dangerous to himself or the person of another or others and that disclosure of information about the condition of the patient is necessary to prevent threatened danger, he or she, specially designated by the board of the hospital or health-care facility for the purpose, may disclose that information without the consent of the patient.

24. That when a senior official of a hospital or health-care facility or a physician, believes, on reasonable grounds, that a patient has been a victim or the perpetrator of a crime, he or she may so inform the police without the patient's authorization.

Implementing these recommendations will not eliminate dilemmas. A difficult task will remain for the hospital and physician to select the form of intervention most consistent with upholding the rights and needs of the patient and society. This will vary with the circumstances. The forms of intervention will include taking action to commit the patient, advising the police or other appropriate authorities, contacting the party or parties threatened, and involving an existing support system to assist in monitoring the patient's behaviour, to mention a few of the options. My study has convinced me that hospital employees and physicians can withstand pressure and even threats from the police and be relied on to make a sound

judgment about when information ought to be imparted to the police after weighing all the relevant factors. There is no basis in experience for a fear that the discretion being suggested will be abused. Confidentiality will continue to be the rule. Disclosure without patient authorization will be made only after serious consideration of the interests of the patient and society at large. In the case of hospitals, this discretion cannot, of course, be vested in every employee. The board of every hospital should become involved in analyzing the criteria justifying disclosure and should create guidelines. The authority to release health information without a patient's authorization should be given only to the hospital administrator or a senior employee designated by him or her in writing.

#### *Recommendations:*

25. (1) *That administrators of hospitals and health-care facilities, or senior employees designated by them in writing, be the only persons permitted to disclose health information from the records of their respective facilities, or in the possession of employees of those facilities, to the police without patient authorization.*

(2) *That before disclosure is made, steps be taken to ensure that the person seeking the information is, in fact, a police officer by requiring the police officer to attend personally at the hospital or health-care facility, or by using a call-back system.*

(3) *That a log be maintained at every hospital and health-care facility, to record the date of the request, the name of the inquirer, his or her police force, his or her badge number, the patient about whom the information was sought, the purpose for which the information was sought, whether information was provided or denied and the substance of the information provided.*

26. That every hospital and health-care facility in Ontario be required to report yearly to the Minister of Health the number of police attendances for confidential information, in general terms, the circumstances in which the information was sought, the number of occasions on which information was given and the number of occasions on which it was refused. The Minister of Health should make these statistics public.

No physician's employee should be permitted to disclose to the police information from physicians' records without patient authorization. Only the treating physician or his or her successor in practice should have that right. It would be a desirable practice for The College of Physicians and Surgeons of Ontario to encourage physicians to keep a record of all requests for information by the police and their disposition.

To limit the right of physicians and hospitals to disclose information to the police to cases where patients are potentially harmful would be unsatisfactory. Surely, they should be equally free to inform the police of their opinions that their patients pose no threat of harm to anyone or were not involved in a crime.

Elsewhere in this report the right of patients to access to their own health information is supported. It is right that, in the context of the present discussion, I should add the expression of my view that the right of access cannot be absolute. I do not believe that the fact that information of the kind I have been discussing has been disclosed to the police by a patient's hospital or physician need itself be disclosed to the patient. Many of the situations in which police seek health information without authorization involve bizarre conduct by patients who are often sick and, sometimes, even prone to violence. It was, it will be recalled, partly for this reason that I concluded that the names of the nine psychiatrists who had released information to the police without their patients' authorization ought not to be disclosed. For the same reason, it would not be appropriate to compel hospitals and physicians to record in the patients' records the fact of the contact with the police and the substance of the information disclosed.

*Recommendation:*

27. That hospitals, health-care facilities and individual health-care providers not



*be obliged to record in their patients' records the fact of any contact with the police or the substance of any information given to the police in cases in which patient information has been given to the police without the patients' authorization.*

The discretion being recommended should not be thought to imply support for the creation of an intimate relationship between physicians and hospitals on the one hand, and the police on the other. The rule of confidentiality of health information must continue to prevail. Departure from the rule can only be countenanced in exceptional circumstances. I am confident that the discretion to be entrusted to hospitals and physicians will be carefully and wisely used.

## Health-Care Workers and Subpoenas

How health-care providers ought to respond to a subpoena in criminal cases is a question that arose during the inquiry. Certainly, once he or she is a witness, that is, is actually testifying, to speak the truth is an absolute requirement. But what is his or her duty while under subpoena but not yet a witness? For example, may a physician speak fully and frankly and provide health information about his or her patient, without the patient's consent, to the investigating police officer assisting the Crown Attorney in a criminal case in which the patient is accused? This problem, of course, also occurs in a civil case. For example, a physician may be subpoenaed by a party adverse in interest to the patient and the lawyer for the patient's adversary may want to discuss the patient's health history with him or her before he or she is called upon to testify at a civil trial in which the patient's health is a relevant issue. My answer is that physicians ought not to be permitted to discuss their patients' health before testifying, without the patient's authorization, even though under subpoena.

In the situations in which I recommended that a discretion be vested in physicians to disclose health information about their patients without the patients' authorization, an emergency of some proportion was always involved. Only the existence of an emergency justifies nonauthorized disclosure. If a party who has served a subpoena on a physician or on the custodian of a hospital's medical record desires a court to hear or read confidential health information about the adversary, he or she need simply call the person served with the subpoena to the

witness box. Once a witness, that person is charged with the duty of speaking truthfully. To adopt a rule permitting a physician or medical record administrator to speak fully, freely and candidly about the patient's health, without the patient's authorization, upon being served with a subpoena, would be to encourage the use of the subpoena as a means of embarking on a fishing expedition. It has not been demonstrated that the needs of modern litigation require this sort of invasion of privacy. In civil matters, discovery techniques make further departures from the rule of confidentiality unnecessary. I endorse the view expressed by Judge Charles A. Waters, of the Common Pleas of Philadelphia County, Pennsylvania, in Alexander et al. v. Knight (1962), 177 A.2d 142 at page 146:

We are of the opinion that members of a profession, especially the medical profession, stand in a confidential or fiduciary capacity as to their patients. They owe their patients more than just medical care for which payment is exacted; there is a duty of total care; that includes and comprehends a duty to aid the patient in litigation, to render reports when necessary and to attend court when needed. That further includes a duty to refuse affirmative assistance to the patient's antagonist in litigation. The doctor, of course, owes a duty to conscience to speak the truth; he need, however, speak only at the proper time.

#### *Recommendation:*

28. That, on receipt of a subpoena or any other process requiring an individual health-care provider, or the custodian of a medical record in a hospital or health-care facility, to attend to give evidence, he or she not disclose health information, without the patient's authorization, in advance of, or in preparation for, his or her attendance as a witness in the proceeding.

## The OPP Registration Branch

The Registration Branch of the Ontario Provincial Police is responsible for the regulation of private investigators under

the provisions of The Private Investigators and Security Guards Act, R.S.O. 1970, chapter 362.

In the discussion, elsewhere in this report, of Centurion Investigation Ltd., there will be found a detailed account of the telephone pretexts made by a Centurion investigator to The St. Catharines General Hospital in an unsuccessful attempt to obtain confidential health information about a patient, one J.M. The pretexts were misrepresentations that the first caller was a nurse at a Toronto hospital, and that the second was a physician, a "Dr. Henderson". It was our discovery of this pretext that led to the disclosure that Centurion Investigation Ltd. had been obtaining confidential health information from hospitals, physicians and their employees by pretext for casualty insurers. J.R. Barr, Q.C., the solicitor for The St. Catharines General Hospital, reported particulars of this incident to the OPP on May 14, 1977. The OPP investigation carried out by the Registration Branch revealed that Paragon Investigation Ltd. had been retained by Wawanesa Mutual Insurance Company to carry out an investigation of J.M.'s medical condition. The Registration Branch was unable to prove to its satisfaction who had made the calls to the hospital although, as Staff Sergeant Merlin Stroud testified, the OPP believed that the call originated with Centurion Investigation Ltd.

Paragon Investigation Ltd. was a company controlled by the McGarry brothers, who also controlled Centurion Investigation Ltd. Paragon Investigation Ltd. surrendered its licence. Acting Superintendent James Villemaire testified that the surrender of the Paragon licence did not end the investigation of Centurion Investigation Ltd. However, no members of the Registration Branch reviewed Centurion Investigation Ltd.'s files to determine whether calls of a similar type had been made, despite the fact that The Private Investigators and Security Guards Act conferred the power to undertake a review since a complaint had been made. The failure to carry out a review of this kind was never satisfactorily explained. It is my conclusion that, for all practical purposes, the surrender of the licence by Paragon Investigation Ltd. terminated the OPP investigation. I am satisfied that Paragon Investigation Ltd. surrendered its licence in the hope--a hope that was realized--that the surrender would put an end to the investigation and thereby protect from disclosure the practice by Centurion Investigation Ltd. of obtaining access to health records of claimants without their authorization.

As I have shown elsewhere, the evidence disclosed that investigators from investigation firms operating in Ontario sought, usually with success, confidential health information

without patient authorization, not only from physicians, hospitals and insurers but also from school board employees, school nurses, the Workmen's Compensation Board, the Unemployment Insurance Commission, OHIP, police forces, employers and various government agencies, including probation service officers, Immigration Department investigators, municipal and social assistance departments, the Ministry of Community and Social Services and the Ministry of Transportation and Communications. In short, no source of information was safe from these investigators.

Despite the existence of the Registration Branch and its considerable powers, the private investigation industry in Ontario was out of control. The Registration Branch did not even report The St. Catharines General Hospital incident to this inquiry despite its obvious relevance. We discovered it during a survey of all public hospitals. The state of the Registration Branch is best illustrated by the fact that, on one occasion, C.C.R., a private investigation firm, was able to obtain extracts from the Registration Branch's file relating to a licensed investigator whom C.C.R. was retained to investigate. The C.C.R. report reads, in part, as follows:

We first checked with the registration department of the Ontario Provincial Police which is responsible for the licencing and policing of security guard and investigation companies in this Province.

A confidential source contacted there supplied the following information from Mr.           's record.

Mr.           was born in Holland on February 20th, 1911 in the City of Amsterdam. He came to Canada in August 1959.

Although our source there indicated that the information regarding employment came from his application to S.I.S. Protection Company, the O.P.P. appeared to have some more details regarding his employment than those contained on the application form to S.I.S., a copy of which is enclosed. You will note on the S.I.S. application form that           lists his employment from September 1959 through to November 1968.

There are gaps in the period of employment listed on the S.I.S. application form, and presumably these were filled in in the course of the O.P.P. investigation of for his licence to be employed as a Security Guard. They do not, however, show his employment further back than 1962.

We draw your attention to the fact that on the S.I.S. application form lists his first employment in Canada as lasting until August 1961. However, his next employer, he indicates, was not until May of 1963, this being the Company of Canada on in . There is no explanation for this gap of almost two years. Again, there is a gap in employment as indicated on his S.I.S. application form from June 1967 to January 1968. You will note that claims to have been employed at on Road in Mississauga up to November 1968 and his reason for leaving there, he has listed as car accident. We draw your attention however, to page 1 of his S.I.S. application form where there is a question which asks if the applicant has ever had a serious illness or serious accident. did not answer this question nor did he supply details as requested in the followup question to that.

The O.P.P. source supplied an employer not listed on 's application form and this is a company which they show as Company on Road. According to the O.P.P. indicated or was verified as having been employed with this company during the period between October 1964 to April 1965. He gave as his reason for leaving this company the fact that the plant had closed. This company as you will note is not mentioned by himself who filled out and signed the S.I.S. application form.

According to the O.P.P. records, was employed with Canada in or between September 1962 to September 1964 and this conflicts with the information given by himself on his own application form.



Also, according to the O.P.P. records, claimant worked for the Government of Canada at the Department of on Street in Toronto during the period of between December 1966 to June 1967. Again there appears to be a discrepancy here between the O.P.P. records and 's own statement. The O.P.P. records also show that he was employed with , Road, Toronto between April 1965 and October 1966. His reason for leaving this, as also was his reason for the change from the Department job, was that the job was finished.

was granted a licence to be employed as a security guard with the S.I.S. Company and was employed with them from September 10th, 1971 to December 14th, 1971. His reason for leaving S.I.S. was listed only as "Resigned".

There is no employer listed according to the O.P.P. between the period 1968 and September 1971 when applied for the job with S.I.S. There is nothing on the O.P.P. records to show any explanation for this gap in his employment, but neither is there any comment to the effect that he was disabled during this period and unable to work.

We checked local reference books and the current telephone book for any listing for a company called and at Avenue in , or in fact at any address, but find no listing for any company by this trade style. We also checked the current City Directory for 1973 and it shows no such address as Avenue in New Toronto.

The same is also true of .

There is nothing to indicate any violations of licence requirements as covered under the act governing the licencing of investigators or security guards. The O.P.P. has had no occasion since left S.I.S. to conduct

any investigations on the claimant or to be interested in his present employment.

From this they assume that he is not working in the security field, and has not done so since 1971 when he resigned from S.I.S.

The important question is why the Registration Branch functioned so inefficiently. Part of the answer is that it had insufficient manpower. In 1977, the Registration Branch was attempting to regulate the investigation industry with only six full-time employees and ten civilians while being responsible for the supervision of 295 investigation companies and 48 security guard agencies, which employed 13,238 security guards and private investigators. The Registration Branch was responsible for licensing each of those persons and firms annually. It carried out this responsibility manually. It was only in January, 1978 that a computer was installed to lighten the paper load. Furthermore, the Registration Branch seems to have viewed its function primarily as an automatic licensing bureau. It did not, it appears, consider itself a regulatory agency concerned with policing breaches, not only of the law relating to confidentiality, but of all the laws affecting the entire range of an investigator's activities. In short, the Branch focused primarily on its administrative functions and relegated its investigative functions to a secondary position.

The Private Investigators and Security Guards Act permits the Registrar of the Registration Branch to inspect an investigator's records only when a complaint is made. Section 17 of the Act provides as follows:

(1) Where the Registrar receives a complaint in respect of the carrying on of the business of providing private investigators or security guards and so requests in writing, the person carrying on the business shall furnish the Registrar with such information respecting the matter complained of as the Registrar may require.

(2) For the purposes of subsection 1, the Registrar or any person designated in writing by him may at any time make an inspection of the books, documents and records of any licensee.

(3) Upon an inspection under subsection 2, the person inspecting is entitled to free

access to all books of account, cash, documents, bank accounts, vouchers, correspondence and records of every description of the licensee, and no person shall withhold or destroy, conceal or refuse to furnish any information or thing required by the person inspecting for the purposes of the inspection.

The fact that the Registrar required a complaint before being able to inspect an investigator's records, as I have suggested, in part explains the failure to initiate investigations but, it does not explain why, as in the case of The St. Catharines General Hospital incident, once a complaint had been made, a thorough investigation was not carried out and acted upon. The failure of the Registration Branch properly to regulate the private investigation industry occurred because the Branch was an understaffed, overworked, and overextended unit, which, under the existing legislation, did not have the power to initiate investigations without a complaint, or, of its own initiative, to inspect private investigators' records.

One of the solutions to this problem that had to be considered was the removal of the responsibility for the regulation of the private investigation industry from the OPP. That raised the question of an alternative. One is the creation of an agency independent of the OPP. After much deliberation and soul searching I rejected this alternative. To begin with, a regulatory agency already exists. More important, the OPP has the greatest reservoir of investigation expertise in Ontario and has the capability of supervising the private investigation industry properly if it could allocate sufficient manpower to do so. The OPP should continue to have the responsibility for the regulation of the private investigation industry. In reaching this conclusion, I take some comfort in the OPP's expressed recognition that insufficient resources had been allocated to the regulation of the private investigation industry. The evidence is that the force has taken and is continuing to take steps to remedy this situation by installing a computer facility, allocating new and increased manpower, and instituting reorganization in the structure of command.

#### *Recommendations:*

29. *That the responsibility for the regulation of the private investigation industry remain with the Registration Branch of the Ontario Provincial Police.*

30. That the Ontario Provincial Police allocate sufficient manpower and expertise to regulate the private investigation industry properly.

The Private Investigators and Security Guards Act requires amendment. The Registration Branch should be given the power to inspect the files of investigators even in the absence of complaint. Without this power, it will be difficult for the Registration Branch to regulate the industry adequately. Members of the Registration Branch have an obligation to keep confidential information they receive during their inquiries. They must clearly be prohibited from communicating any information received in the course of their inquiries to police officers in other branches of the force or any other forces. I accept the evidence given at our hearings that members of the Registration Branch will not disclose confidential information to other members of the force. Confidentiality of information is most sensitive and could easily be subject to abuse, without constant vigilance, in situations in which investigators are retained to carry out investigations for lawyers acting for the defence in criminal matters. In these circumstances, the obligation of investigators to maintain records should not extend to the notes and reports to any lawyer acting in that capacity, provided that these notes and original reports are delivered to that lawyer.

*Recommendations:*

31. That The Private Investigators and Security Guards Act be amended to allow the Registration Branch to inspect investigators' records and reports even in the absence of a complaint.
32. That the members of the Registration Branch be under an obligation of confidentiality with respect to the contents of the investigators' files inspected, and be required to refrain from disclosing any information acquired during inspection of investigators' files to officers in other branches of the OPP or officers of any other force, and to use this information only for the purposes of registration hearings or for the prosecution of any breaches of the law.

33. *That private investigators have an obligation to maintain books, records and copies of all reports. This obligation should not apply in situations in which investigators are retained by lawyers acting for the defence in criminal or quasi-criminal matters. In those circumstances, the defence lawyer involved should be permitted to take custody of all notes, records and reports relating to the case.*

## Search Warrants

The last matter to be discussed is that of search warrants obtained by police officers for execution against hospitals permitting the seizure of hospital records. In some criminal investigations search warrants are issued, directed to public hospitals and to psychiatric facilities operated by the Ministry of Health, and authorizing the seizure of specified documents and records. A search warrant permitting the seizure of documents and records relating to a particular patient is usually unobjectionable. However, warrants have sometimes been issued requesting only "hospital records" and on two occasions, search warrants were issued, directed to the Whitby Psychiatric Hospital authorizing the seizure of:

Records of absenteeism, leaves and elopees  
pertaining to 11, 12, Aug. 1978;

. . . . .

Hospital records of discharges, leaves of absence (with or without permission) and other pertinent documents and records of absences of all patients of Whitby Psychiatric Hospital on June 29, 30, July 1, 2, 1979 inclusive.

Public hospitals, as corporations are, in law, independent of the Ministry of Health. Public hospitals usually retain solicitors who deal generally with the hospitals' legal matters. A hospital is therefore able to obtain independent advice from its solicitor with respect to the validity of warrants directed to it. In seeking advice about the validity of a search warrant the hospital is concerned to maintain the integrity and confidentiality of its patients' records.



Whitby Psychiatric Hospital is, as I have said, a psychiatric facility operated by the Ministry of Health. The Ministry of Health also operates psychiatric facilities at Brockville, Hamilton, Kingston, Thunder Bay, London, North Bay, Penetanguishene, Toronto and St. Thomas. The administrators of these psychiatric facilities have express instructions to seek legal advice in any case in which they have any doubt about the validity of a search warrant directed to their institution. This advice is sought from solicitors in the Legal Branch of the Ministry of Health. Although, from an organizational point of view, these solicitors are members of the Attorney General's Ministry, their sole function is to provide legal advice to the Ministry of Health.

The competence of these solicitors to give sound advice to the administrators of the various provincial psychiatric facilities to protect the confidentiality and integrity of the facilities' patients' records is undoubted. David Bernstein, Q.C., the Director of the Legal Branch of the Ministry of Health, in a letter dated December 12, 1979, quite accurately described the relationship between the solicitors in the Legal Branch of the Ministry of Health and the Ministry of the Attorney General.

As you know, counsel in this Ministry's Legal Branch are members of the Attorney General's Ministry (Common Legal Services). Our function is to provide legal advice and services to the Ministry of Health.

I consider that, in any circumstances where the interests of the Ministry of Health are inconsistent with the interests of the Ministry of the Attorney General--for example, in a conflict between expedient law enforcement and a duty of confidentiality--the duty of this Branch is owed solely to our client Ministry. It is no part of our function to promote the interests of the Attorney General, in any case of conflict between the two Ministries. I have always understood that this was laid down by the Attorney General's Ministry when all Ontario Government lawyers became part of that Ministry (about 1972/73), and have never received any direction or comment to the contrary effect.

The difficulty with which I am concerned is best illustrated by a consideration of two warrants directed to the Whitby Psychiatric Hospital. In my opinion, the language of the warrants is so broad in the description of the documents sought that there is good reason to doubt the validity of the warrants. What is important, however, is the process by which the decision is arrived at on the question of the proper response to the warrants to be made by the hospital. Mr. Bernstein's letter explains:

In the two Whitby cases mentioned above where the subject matter of the warrant did not relate to a specified patient, the Administrator of the Hospital telephoned us for advice.

1. As to the warrant of December 18, 1978 the counsel who received the call was not familiar with the legal requirements for a valid search warrant and sought advice (also by telephone) from the Crown Law Office Criminal. The opinion given to him was that the warrant was not objectionable simply because it did not identify specific patients. Acting on this advice, counsel advised the Administrator that he should accede.

2. As to the warrant of July 11, 1979 the counsel receiving the call (not the same counsel as in the previous case) also contacted the Crown Law Office Criminal. Again, he was advised (orally) that the warrant was not objectionable. Counsel disputed that advice. The question then arose as to whether, if the Hospital decided to contest the validity of the warrant, the Attorney General's Ministry would represent the Hospital on the Motion to quash (as you know, that Ministry customarily represents the various sections of the Government in judicial proceedings); their advice was that, given their responsibilities in the area of law enforcement, it would be a conflict of interest for the Attorney General to represent the Hospital on the Motion.

As it happened, before it became necessary for the Hospital to launch the Motion a suspect was apprehended and the warrant was not pursued further.

The lawyers in the Crown Law Office of the Ministry of the Attorney General work in close co-operation with the police. It is inappropriate for the Legal Branch of the Ministry of Health to seek an opinion from the Crown Law Office with respect to the validity of a search warrant, for to do so could appear to place the lawyers in the Crown Law Office in a conflict of interest position. In the event that the lawyers in the Legal Branch of the Ministry of Health believe that they should have another opinion about the validity of search warrants or, for that matter, about anything else that relates to the issues of confidentiality and the police, the prudent course would be to retain outside counsel rather than to seek an opinion, whether formal or informal, from lawyers in the Crown Law Office.

*Recommendation:*

34. *That in the event that the Legal Branch of the Ministry of Health desires another legal opinion with respect to the validity of a search warrant or any other process directed to provincial psychiatric facilities, the opinion should be sought from a non-government lawyer rather than from the Crown Office.*

All provincial psychiatric hospitals now keep a record of all search warrants executed against them. This is a salutary practice that should be adopted by all hospitals and health-care facilities.

*Recommendation:*

35. *That all hospitals and health-care facilities keep a record of all search warrants executed against them.*

## APPENDIX I

### CABINET DIRECTIVE NO. 35

#### Security in the Public Service of Canada

##### POLICY

1. Security in the public service of Canada is essentially a part of good personnel administration, and therefore it is the responsibility of each department and agency. The security of classified information in the possession of a department or agency may be placed in jeopardy either by persons who may be disloyal to Canada and her system of government or by persons who are unreliable because of defects in their character.
2. Employees in the public service of Canada, including members of the Armed Services and the Royal Canadian Mounted Police, who are required to have access to classified information in the performance of their duties, must be persons in whose reliability and loyalty to his country the Government of Canada can repose full confidence. It has been clearly demonstrated that such confidence cannot be placed in persons whose loyalty to Canada and our system of government is diluted by loyalty to any Communist, Fascist, or other legal or illegal political organization whose purposes are inimical to the processes of parliamentary democracy. It is therefore an essential of Canadian security policy that persons described in paragraph 3 below must not, when known, be permitted to enter the public service, and must not if discovered within the public service be permitted to have access to classified information. If such a person is in a position where he has access to classified information, he must at least be transferred to a less sensitive position in the public service. It may also be necessary, where it appears to the Minister concerned to be in the public interest, to dismiss him from the public service, subject to the conditions set out at paragraph 17 below.
3. The persons referred to in paragraph 2 above are:
  - (a) a person who is a member of a communist or fascist party or an organization affiliated with a communist or fascist party and having a similar nature and purpose;

- (b) a person who by his words or his actions shows himself to support a communist or fascist party or an organization affiliated with a communist or fascist party and having a similar nature and purpose;
- (c) a person who, having reasonable grounds to understand its true nature and purpose, is a member of or supports by his words or his actions an organization which has as its real objective the furtherance of communist or fascist aims and policies (commonly known as a front group);
- (d) a person who is a secret agent of or an informer for a foreign power, or who deliberately assists any such agent or informer;
- (e) a person who by his words or his actions shows himself to support any organization which publicly or privately advocates or practices the use of force to alter the form of government.

4. It must be borne in mind that there may be reason to doubt the loyalty of a person who at some previous time was a person as described in paragraph 3 above, even though this doubt may not be confirmed by recent information about him.

5. In addition to loyalty, reliability is essential in any person who is to be given access to classified information. A person may be unreliable for a number of reasons that do not relate to loyalty. To provide as much assurance of reliability as possible persons described in paragraph 6 below may not be permitted to have access to classified information, unless after careful consideration of the circumstances, including the value of their services, it is judged that the risk involved appears to be justified.

6. The persons referred to in paragraph 5 above are:

- (a) a person who is unreliable, not because he is disloyal, but because of features of his character which may lead to indiscretion or dishonesty, or make him vulnerable to blackmail or coercion. Such features may be greed, debt, illicit sexual behaviour, drunkenness, drug addiction, mental imbalance, or such other aspect of character as might seriously affect his reliability;



- (b) a person who, through family or other close continuing relationship with persons who are persons as described in paragraphs 3(a) to (e) above, is likely to be induced, either knowingly or unknowingly, to act in a manner prejudicial to the safety and interest of Canada. It is not the kind of relationship, whether by blood, marriage or friendship, which is of primary concern. It is the degree of and circumstances surrounding such relationship, and most particularly the degree of influence that might be exerted, which should dictate a judgment as to reliability, a judgment which must be taken with the utmost care; and
- (c) a person who, though in no sense disloyal or unreliable, is bound by close ties of blood or affection to persons living within the borders of such foreign nations as may cause him to be subjected to intolerable pressures.

7. In addition it must be recognized that there may be a serious risk to security in employing or permitting to be employed persons such as those described in paragraph 3 or 6 above:

- (a) in certain positions in industrial firms and related establishments involved in or engaged upon the production or study of classified defence equipment which requires security protection; or
- (b) in positions in government organizations engaged in work of a nature vital to the national security which, although they do not normally involve access to classified information, may afford their incumbents opportunities to gain unauthorized access to such information.

8. To carry out their responsibility for the safekeeping of the secrets of the Government of Canada and her allies, departments and agencies must first obtain sufficient information about a person to be given access to these secrets in order that a reasonable judgment might be made as to his or her loyalty and reliability. In making this administrative judgment, it must always be borne in mind that, while the interests of the national security must take precedence where there is a reasonable doubt, the safeguarding of the interests of the individual is also essential to the preservation of the society we seek to protect. Information bearing on the security status of an employee will be treated as confidential.

## PROCEDURE

9. The following procedures by which this policy is to be implemented are designed to provide that the most careful screening possible be given, particularly to persons who will have access to highly classified information. It is the continuing responsibility of each government department and agency to ensure that its security remains unimpaired.
10. Information about persons who are being considered for access to classified information must be obtained at least from the persons themselves, from referees named by the persons, and from investigations conducted by authorized investigative agencies. Departments and agencies will inform persons who are being considered for access to classified information of the reasons for seeking background information about them, and to explain to them the dangers to themselves as well as to the national security in their attempting to conceal any information which may have a bearing on the degree of confidence that can be reposed in them.
11. The functions of an investigative agency are to conduct promptly and efficiently such investigations as are requested by departments or agencies to assist them in determining the loyalty and reliability of the subject of investigation; and to inform departments and agencies of the results of their investigations in the form of factual reports in which the sources have been carefully evaluated as to the reliability of the information they have provided.
12. On the basis of these reports and such other pertinent information as has been obtained from the person concerned, from the character references which he has given, and from such other sources of information as may have been utilized, the employing department or agency will arrive at a considered judgment of the person's loyalty and reliability, and of the degree of confidence that can be reposed in him to carry out safely and efficiently the duties to be performed.
13. If a favourable determination is made, the department or agency may grant a security clearance to the level required for the efficient performance of the duties of the position concerned. If, on the other hand, there is in the judgment of the deputy minister of the department or the head of agency concerned a reasonable doubt as to the degree of confidence which can be reposed in the subject, the

granting of a security clearance will be delayed until the doubt has been resolved to the satisfaction of the deputy minister or the head of agency.

14. Where an applicant for employment in the public service, as opposed to a person already employed, is being considered for appointment to a position requiring access to classified information and doubt has arisen as to his suitability for such access, the following courses of action may be taken with a view to resolving that doubt:
  - (a) further specific investigation may be requested of an authorized investigative agency; or
  - (b) the department or agency may at any time seek the advice of the Interdepartmental Security Panel.
15. Where a person is already employed in the public service, and a doubt has been raised as to his suitability to have access to classified information, the security officer of the department or agency must take such action as is necessary to preserve security and may take the courses of action referred to in paragraph 14 with a view to resolving that doubt. Should these actions fail to resolve the doubt, or appear to the department or agency to be inexpedient under the circumstances, the assistance of the employee himself shall be sought in an attempt to resolve the doubt. A senior officer appointed by the deputy minister or head of agency shall, after appropriate consultation with the investigative agency or other source of the information which raised the doubt, interview the subject and inform him, to the fullest extent that is possible without jeopardizing important and sensitive sources of security information, of the reasons for doubt, and shall give the employee an opportunity to resolve it to the satisfaction of the responsible department or agency.
16. Should none of the courses set out in paragraph 15 above result in a satisfactory resolution of doubt concerning a government employee, the responsible department or agency shall withhold a security clearance, shall take such action as is necessary to preserve security and shall consult the Secretariat of the Security Panel with a view to their assisting the department or agency in determining tentatively:
  - (a) whether the subject might safely and usefully be appointed to a less sensitive position in the department or agency or elsewhere in the public service, with his

knowledge and consent to the fullest degree possible under the circumstances;

- (b) if appointment elsewhere is not possible, whether he should be asked to resign his position in the department or agency; or
- (c) if he refuses to resign, whether it should be recommended to the Minister responsible that the person be dismissed from the public service.

17. Should the department decide that a recommendation for dismissal should be made, no action shall be taken on such recommendation until:

- (a) the deputy minister or head of agency has personally made a complete review of the case, and has himself interviewed the employee in question, in a further attempt to resolve any reasonable doubt as to his trustworthiness;
- (b) the employee has been advised, to the fullest extent possible without jeopardizing important and sensitive sources of security information, why doubt continues to be felt concerning his loyalty or reliability, and has been given a further opportunity to submit any information or considerations that he thinks ought to be taken into account on his behalf by the deputy minister or head of agency; and failing a satisfactory resolution,
- (c) the advice of a board of review drawn from the members of the Security Panel has been sought on the basis of all the information available. (The board of review shall consist of the Chairman and at least two members of the Security Panel, with the proviso that no member who is directly concerned with the case shall sit as a member of the board.)

18. In arriving at a final decision as to whether to recommend to the Governor in Council that an employee be dismissed on grounds of security, the Minister responsible will take into account all of the relevant information and advice that has been provided, but the Minister is not bound to act on such advice.

19. The numbers of all persons who for security reasons are removed from eligible lists by the Civil Service Commission, or are in one way or another refused access to classified

information by departments or agencies for security reasons, will be sent quarterly to the Secretary of the Security Panel in order that the Panel may from time to time review the number of persons or the type of cases involved, and assess the extent of the security problem in the public service. The figures provided should be broken down in the following general categories: persons dismissed, persons permitted to resign, persons transferred to non-sensitive posts, persons denied access to classified information, persons denied employment. In addition the figures should indicate whether the action was taken on grounds of disloyalty or unreliability. Figures should not include persons who are no longer given access to classified information because of a change in duties or other similar administrative reasons.

20. It is the responsibility of each deputy head, or head of an agency, to nominate a competent senior official, preferably the Senior Personnel Officer, to act as security officer, and to notify the Secretary of the Security Panel of the appointment and of any subsequent change. The official so nominated shall be cleared for security in accordance with the procedures set out in paragraph 25(i) below. The person so named will be responsible to the deputy head or head of an agency for ensuring that all regulations relative to security are carried out within the department or agency. It will also be the responsibility of the departmental security officer to maintain close liaison with the government agencies responsible for security policy and procedures. It is important that wherever possible security officers should be persons who may be expected to continue their work over a long period of time, since effective security is difficult to maintain without considerable experience in a specialized field.

## METHODS

21. Security screening of applicants to the public service will be initiated by the Civil Service Commission, or by departments and agencies in the case of persons not employed under the Civil Service Act. Where persons already employed in a department or agency are to be given access to classified information, security screening will be initiated by the department or agency concerned.
22. When it appears necessary on security grounds for the Civil Service Commission to reject an applicant, or a candidate for a position involving access to classified information



who is already in the public employ, the Commission will when appropriate consult with the interested department in order to reach a joint agreement as to what action may finally be taken, bearing in mind the fact that the ultimate responsibility for security rests with the department.

23. When it appoints to a department a new employee who has been the subject of a security screening, the Civil Service Commission will send forward to the department all the pertinent information and documentation relating to the security screening.
24. A person to be appointed to a permanent position in the public service will not normally be made the subject of security screening for this reason alone. But whenever a person to be appointed to such a position is, in the opinion of the deputy minister or head of agency concerned, likely to be required eventually to have access to classified information, that person shall before being given a permanent appointment, be made the subject of a fingerprint and file check if this has not already been done.
25. Within the policies and procedures set out above, a security assessment and clearance will be made by the following means. These represent security criteria and methods which are consistent with present investigative services available interdepartmentally; they are minimum standards and do not limit in any way the right of the armed forces to conduct field checks, through their own resources, of personnel employed with or on behalf of the Department of National Defence.
  - (i) Persons to have access to Top Secret information

Before a person is employed in a position requiring access to Top Secret information he must be the subject of an investigation in the field by an appropriate investigative agency, his name must be checked against the subversive records of the R.C.M. Police, and he must be the subject of a fingerprint check by the R.C.M. Police. These procedures are mandatory.
  - (ii) Persons to have access to Secret information
    - (a) Before a person is employed in a position requiring access to Secret information his name must be checked against the subversive records of the R.C.M. Police, and he must be the subject of a fingerprint check by the R.C.M. Police. Both these procedures are mandatory.

(b) When the Chairman of the Civil Service Commission or the deputy head of a department or agency, or a security officer appointed by them, considers that information provided by the means set out in paragraph 25(ii)(a) may be clarified by an investigation in the field, or that such an investigation is necessary to satisfy him as to an applicant's or employee's loyalty and reliability, he may request that an inquiry be made of a person's background by a field investigation to be carried out by an appropriate investigative agency. Where it appears that requests from a department or agency dealing with the R.C.M. Police as the investigative agency exceed what seems to be a normal requirement, the R.C.M. Police may ask the Security panel to allot priorities.

(iii) Persons to have access to Confidential information

Before a person is employed in a position requiring access to Confidential information, his name must be checked against the subversive records of the R.C.M. Police, and he must be the subject of a fingerprint check by the R.C.M. Police. Both of these procedures are mandatory.

(iv) Responsibility for granting clearances

The deputy head of a department or agency will be responsible for granting or withholding a security clearance and will assume a continuing responsibility for a person's access to Top Secret, Secret and Confidential information.

26. In addition, departments and agencies are reminded that personal consultation with the references listed by the employee in his Personal History Form may provide useful supplementary information about his character. References should therefore be consulted personally when it appears that a useful purpose would be served by so doing.
27. Comparable procedures set forth in paragraph 25, except those relating to fingerprinting, apply equally to persons employed in defence industry (and certain services related to defence) who may be required to have access to classified information which is the property of the Government of Canada or for the security of which the government is responsible. In defence industry (and certain services related to defence) the procedures will be administered by the Department of Defence Production in accordance with a

separate directive relating to security in defence industry.

## APPENDIX II

### MEMORANDUM FOR DEPUTY MINISTERS AND HEADS OF AGENCY

#### Revised Cabinet Directive on Security

On October 24th, 1963, the Cabinet approved Cabinet Directive No. 35 entitled "Security in the Public Service of Canada", which had been revised in the light of extensive study by the Security Panel and by the Cabinet Committee on Security and Intelligence. The Cabinet also agreed that explanatory statements in relation to changes in security policy and procedure would be made in the House of Commons by the Prime Minister and the Minister of Justice. These statements were made on October 25th, 1963, at the introduction of the 1963-64 estimates of the Department of Justice. As a result of suggestions made during the debate, the Prime Minister directed that the new instructions should not be put in written form until the debate on these estimates had been concluded.

The estimates of the Department of Justice were passed in the House of Commons on December 13, 1963, without debate as they related to matters of security. The Prime Minister has consequently agreed that Cabinet Directive No. 35 might now be distributed for use in all Departments and Agencies of the government, effective immediately, and copies are attached for your retention and that of your security officer.

The most important modifications in the new Directive involve an attitude of much greater frankness with employees whose reliability or loyalty is in doubt, and provide related procedures for reviewing such cases both within the responsible department or agency and if necessary by a Board of Review composed of members of the Security Panel.

In addition to ensuring the security of classified information for which each is responsible, departments and agencies are now required by the Directive

- (a) to inform applicants and employees of the reasons for security investigations, and of the dangers to

themselves and to the national security in their attempting to conceal relevant information about themselves;

- (b) to tell an employee about whom doubt has arisen on security grounds of the reasons for that doubt, insofar as is possible without endangering important sources of security information, and to give him an opportunity to resolve the doubt;
- (c) if the doubt cannot be resolved, to attempt usefully to place the employee in a less sensitive position in the department or elsewhere in the public service;
- (d) if dismissal appears to be the only prudent recourse, to have the case reviewed and the employee interviewed by the deputy minister, to give him a further opportunity to resolve the doubt that has been raised about him; and
- (e) to seek the advice of a Board of Review as described in paragraph 17(c) before a recommendation for dismissal is made to the Minister responsible.

5. In addition, more specific criteria for assessing loyalty and reliability than were contained in Cabinet Directive No. 29 are set out in paragraphs 3 and 6. Related procedures in paragraphs 15, 16 and 17 emphasize the necessity of balancing the preservation of security against the rights and interests of the individual. Comparable procedures with regard to defence industry and certain services related to defence are to be administered by the Department of Defence Production in accordance with a separate directive, as indicated in paragraph 27.

6. Deputy Ministers and Heads of Agency, as well as departmental and agency security officers, are requested to give careful consideration to the means by which these new policies and procedures might best be given effect in their various departments and agencies. Because of the greater care and attention that will be required in their implementation, particularly in the review of individual cases, it is expected that a number of problems will arise which will necessitate discussion and consultation. It is hoped that, after the new Directive has been in effect for six months to a year, it will be possible to arrange a conference of departmental and agency security officers to determine the feasibility and effectiveness of these new measures. In the meantime, any enquiries as to interpretation and

implementation might be directed to the Secretary of the Security Panel.

R.G. Robertson,  
Secretary to the Cabinet.

Privy Council Office,  
Ottawa.

### APPENDIX III

#### MEMORANDUM TO ALL DEPARTMENTAL/AGENCY SECURITY OFFICERS:

Regulations Respecting Enquiries  
Relating to Public Service Employees  
whose Dismissal Has been Proposed in  
the Interest of the Safety or Security of Canada  
and  
Consequential Amendment of  
Cabinet Directive No. 35

#### Background

Following the establishment in 1966 of the Treasury Board as a separate department, amendments were made to the Financial Administration Act in 1967, to clarify and establish the powers of the Board in relation to personnel management. A sub-section was inserted in the amendments to protect the power of the Governor in Council to suspend or dismiss persons "in the interest of the safety or security of Canada". The formulation of the sub-section was such that, in preserving the power of dismissal, it specified that it was to be pursuant to "an inquiry conducted in accordance with regulations of the Governor in Council by a person appointed by the Governor in Council". It appears that the effect of the amendment on existing procedures was not adequately appreciated at the time and no regulations were passed pursuant to the new legislation. The deficiency came to light recently and has now been corrected with the Cabinet approval on March 27th 1975 of appropriate regulations, copy of which is attached for your convenience.

#### Revised Procedure

This recent decision brings a major change to the current and mandatory review procedure of adverse security cases



particularly as it appears in paragraph 17, sub-paragraphs (c) and paragraph 18 of C.D. 35. Under the new regulations, a deputy minister or head of agency who, having personally reviewed an adverse case and interviewed the employee in question, concludes that the continued employment of the person in the Public Service of Canada is prejudicial to the safety or security of Canada shall recommend dismissal to the Governor in Council and the appointment of a commissioner under the Regulations.

The revised procedure for the review of adverse security cases will appear, in the near future, in a fully revised C.D. 35. Meanwhile, any deputy minister or head of agency who wishes to recommend dismissal under the Regulations should contact the Assistant Secretary to the Cabinet (Security and Intelligence) for further details.

P.A. Lemieux,  
Security and Intelligence Secretariat.

Privy Council Office,  
Ottawa.

## The Ontario Health Insurance Plan Computer System

Before and shortly after the creation of this inquiry, a number of events occurred that raised doubts about the adequacy of the security of the computer system used by the Ontario Health Insurance Plan. Allegations had been made in the press that the Royal Canadian Mounted Police had been receiving health information from employees of OHIP which they used to disrupt certain political groups. The Ontario Medical Association was made aware that a large number of discarded OHIP claims cards, bearing confidential medical information, had been shipped out of an OHIP office without first being mutilated in any way. Early in our investigation we discovered that private investigators retained by automobile insurance companies were improperly obtaining health information from OHIP which they were inserting in their reports to their clients. Information was being given to immigration officers by OHIP employees. We learned that the Ontario Provincial Police had quarters in the Toronto District Office of OHIP and were able, if they wanted it, to have complete and unauthorized access to OHIP's health information about almost all Ontario residents.

These events, as I have said, gave rise to the inference that the OHIP system was less secure than it should have been if the requirement of confidentiality, which OHIP was obliged to ensure under The Health Insurance Act, 1972, was to have any real meaning. We therefore decided, in 1978, to engage the management consulting firm of Peat, Marwick and Partners to undertake a comprehensive study of the operation of the Ontario Health Insurance Plan system with the object of identifying the places in the system in which security should be a high priority and those in which there were weaknesses. The discussion that follows is a summary of the Peat, Marwick report that resulted from its study.

A few general observations can be made before turning to the particulars of the study. To identify the weak points in the system is to state the solutions to the problems revealed. It was therefore thought to be unnecessary to make formal recommendations. Some of the weaknesses have already been removed by the evolving nature of OHIP's computer system. To cite one example, the use of direct terminal access to the OHIP

system for enrolment information makes unnecessary the distribution of large amounts of information in hard copy. Other problems have been resolved by the establishment of appropriate procedures designed to ensure that a potential exposure is protected by an appropriate security mechanism. The conclusion is inescapable that mere undertaking of the study resulted in improvements in the security of the system. The insights that were gained from the inspection brought about healthy changes internally. This is not to say that security problems will not continue to exist in the system. The truth is, however, that the greatest security risk is to be found, not in the system's hardware or software, but rather in the persons involved in the system. A constant awareness of the duty to maintain security and an appreciation by those persons of the risks to that security are essential. The mandate for the future, then, is heightened awareness, continued inspection of the procedures and performance of employees, and constant continuing education to enhance employees' awareness of their responsibilities.

The Peat, Marwick study, which describes the OHIP system as it existed in 1978, was divided into the following four phases:

Phase I      The administrative organization and systems surrounding the computerized systems were examined. In addition, the basic OHIP computer subsystems and information flows were documented. A series of charts and supplementary documentation were prepared as part of Phase I describing the following:

1. information flows within the Ministry;
2. computer systems overview;
3. critical information flows;
4. major computer subsystems;
5. the forms used and reports generated;
6. the manual and computer files.

Phase II      The second phase involved a detailed walk-through of the system with Commission counsel. This was used as a means of identifying all major administrative and computer procedures and of identifying and rating the many control points within the system.

The control-point rating process resulted in the identification of 18 critical control points from a total of 89 identified control points.

A comprehensive manual was produced in Phase II which includes an overview of the OHIP system, information flows, computer system overview,

critical information flows, computer subsystems, document descriptions, file descriptions, and control-point descriptions. This manual is the first of two volumes and is entitled, "A Study of the Ontario Health Insurance Plan, Documentation Manual", Volume 1 - May, 1978.

Phase III      This phase consisted of the following activities:

1.    the preparation of a testing methodology to assess the 18 critical control points;
2.    the preparation of control-point testing questionnaires;
3.    the preparation of detailed testing packages;
4.    the conducting of on-site reviews of OHIP district offices and head office.

The information gathered during these reviews was used in evaluating the level of control in existence at each control point. The documentation of Phase III activities comprises Volume 2 of the Documentation Manual - September, 1978.

Phase IV      The final phase consisted of an evaluation of the critical control points and test results and the formulation of conclusions and recommendations.

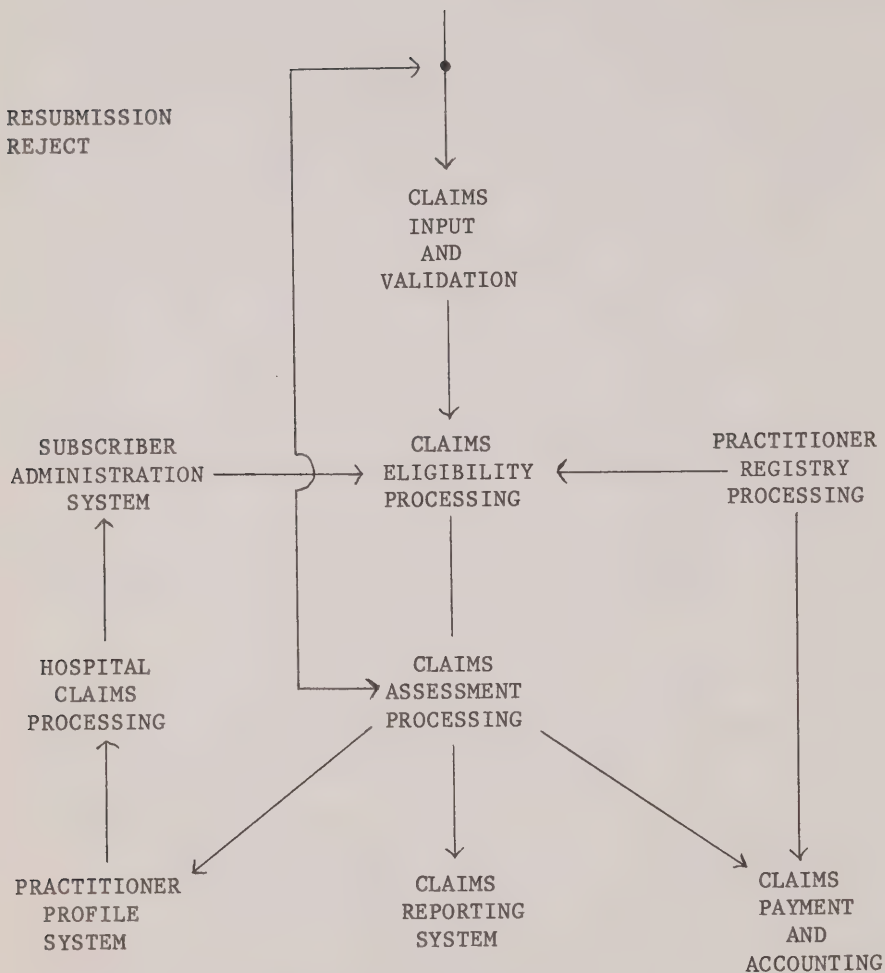
## Major OHIP Subsystems

The OHIP computer system can be subdivided into nine major components or subsystems. The following are the names of the subsystems:

1.    claims input and validation subsystem,
2.    subscriber administration subsystem,
3.    claims eligibility processing subsystem,
4.    practitioner registry processing subsystem,
5.    hospital claims processing subsystem,
6.    claims assessment processing subsystem,
7.    physician/practitioner profile subsystem,
8.    claims reporting subsystem,
9.    claims payment and accounting processing subsystem.

The relationship of OHIP computer subsystems to one another is shown in Figure 1 and each is described in detail below.

FIGURE 1  
OHIP COMPUTER SUBSYSTEMS





## Claims Input and Validation Subsystem

This subsystem is the first step in the claims processing cycle (see Figure 2). Information from claims cards submitted by practitioners to the OHIP district offices is transferred to magnetic tapes. These tapes are submitted by the nine district offices throughout Ontario to the Leaside Data Centre in the Borough of East York where the information on the tapes is entered into the computer system. The processing performed by this subsystem includes the following:

1. Batch checking and balancing in order to ensure that all claims reported by the district offices were in fact coded on tape.
2. Preliminary editing.
3. Matching of resubmitted claims to the corresponding claims on the pending claims file and reconstruction of a corrected claims transaction.
4. Creation of an edited claims file.
5. Updating of the pending claims file with newly rejected claims.
6. Error reporting.

From this subsystem the edited claims file passes to the next step of claims processing, eligibility processing.

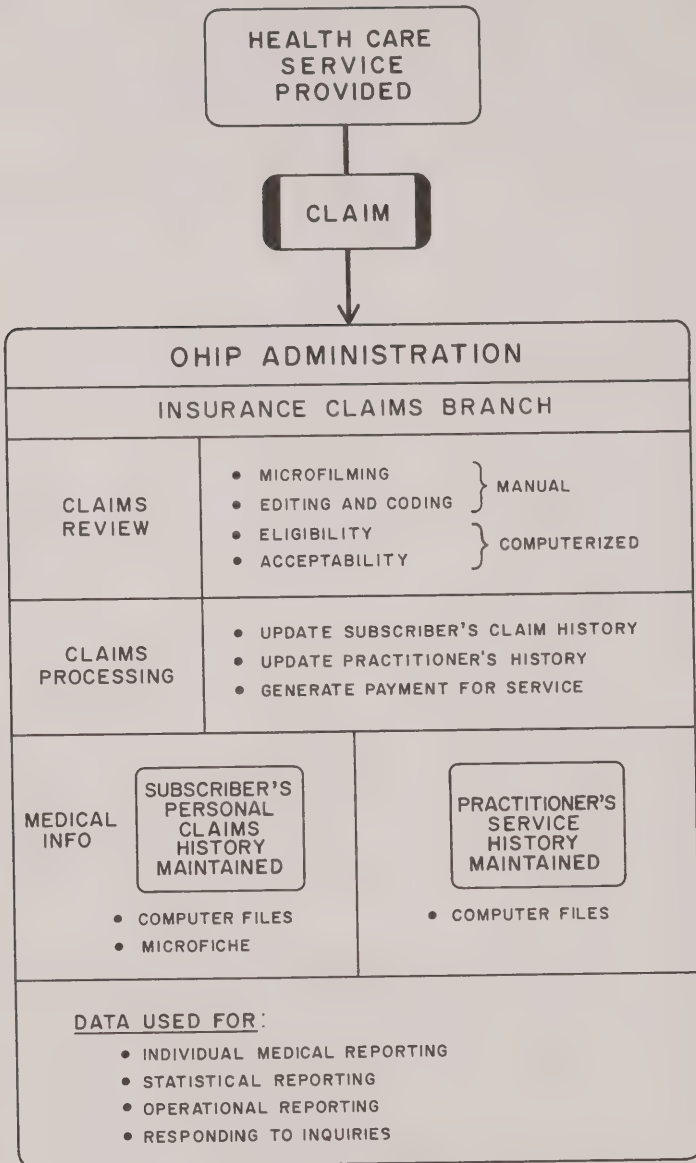
## Subscriber Administration Subsystem

The subscriber administration subsystem maintains enrolment information on all subscribers in the OHIP system. The major file used is called the subscriber data base which is located on magnetic disks.

Information stored on this file is collected by the enrolment branch and includes data on new applicants, changes to current subscriber records, or deletions of subscriber information from the file. In addition, the subsystem records the collection of premiums from subscribers. The premium information is processed against the subscriber data base which records premium payments and triggers the generation of overdue and regular premium notices from the billing data file. Another output of this system is the group checking lists which contain the names of all members of a subscriber group. The lists are

FIGURE 2

# THE CLAIMS PROCESS



forwarded to employers on demand and are used to record any changes in enrolment in a group. The subsystem administers the subscriber information and premium billing processes for both group and pay-direct subscribers.

The subscriber administration subsystem produces two major computer output microfilm (COM) tape files from which the enrolment microfiche are produced. There are two major microfiche files produced by this subsystem. One is kept in numerical order by OHIP number and the other is kept in alphabetic sequence by subscriber surname. Both computer output microfilm tape files contain information on all subscribers in the OHIP system.

## Claims Eligibility Processing Subsystem

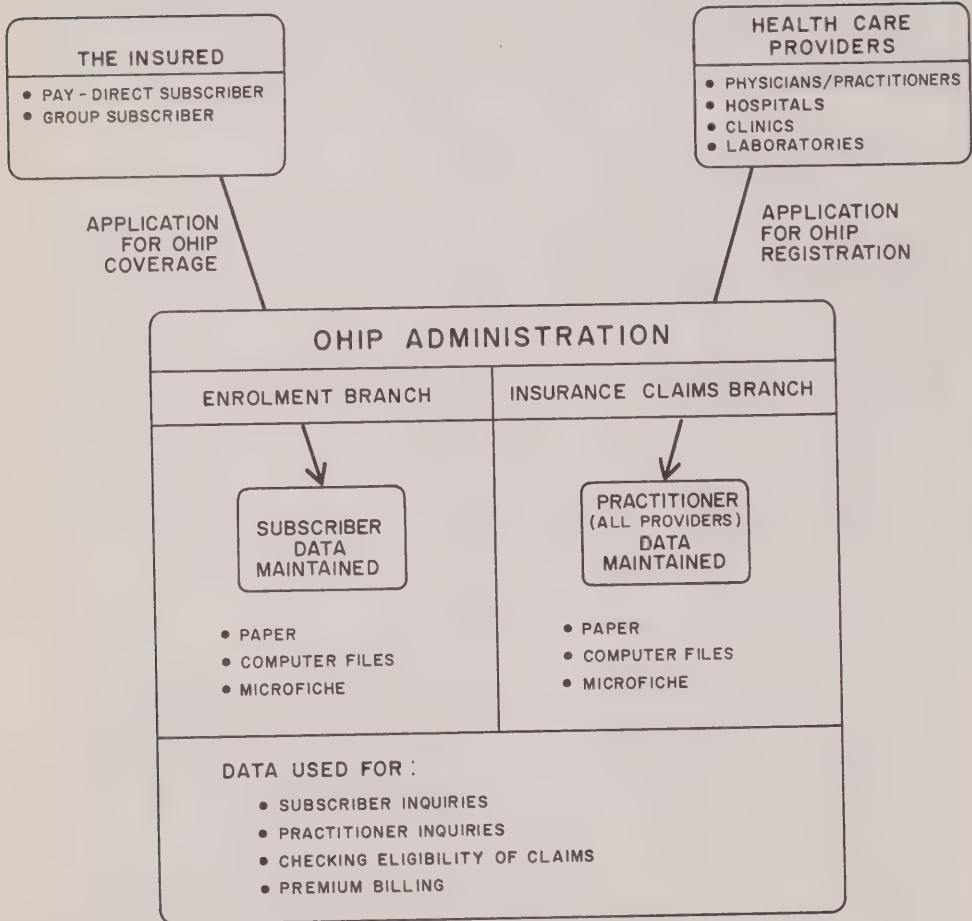
Claims eligibility processing is a two-step process which involves an eligibility check of the subscriber named on the claim and an eligibility check of the practitioner named on the claim. Subscriber eligibility is checked against information on the subscriber data base. Physician or practitioner eligibility is checked against the file of member practitioners called the practitioner directory and against an eligibility master file. The major input to this subsystem is the edited claims file from the claims input and validation subsystem described above. All the claims that fail either of the eligibility tests are shown on a computer file along with the claims that pass the checks and move from this subsystem into the next level of claims processing, which is claims assessment processing.

## Practitioner Registry Processing Subsystem

Like the subscriber administration system, the practitioner registry processing subsystem records the enrolment and registration of physicians and practitioners within OHIP (see Figure 3). There are three major files maintained in this subsystem: the practitioner directory file, the eligibility file and the business practice file. These files are made current by using information submitted to the Claims Services Section of the Insurance Claims Branch. The Claims Services Section is responsible for maintaining the practitioner registration system. Besides producing various reports, the system creates a practitioner registry computer output microfilm tape from which a set of practitioner registry microfiche are created on a regular basis.

FIGURE 3

## THE ENROLMENT PROCESS



## Hospital Claims Processing Subsystem

Hospital claims processing is broken down into the following three major components:

1. admissions eligibility processing,
2. hospital discharge processing,
3. hospital discharge reporting.

### Admissions Eligibility Processing

For every patient entering a hospital the hospital completes an admission report (Form 106A) which it submits to OHIP. The 106A contains the patient's name, OHIP number and an admitting diagnosis. This information is entered onto a magnetic tape and is the major input file to the admission eligibility processing step. The processing involves checking patient information against the subscriber data base in order to confirm that the patient is eligible under OHIP and is therefore not required to pay his or her own hospital expenses. Every eligible admission results in the production of a hospital discharge form (Form 106D) by the computer system, containing the same information that was submitted on the admissions report except for diagnosis. All rejected admissions are submitted to the Eligibility Testing Unit of the Enrolment Branch for further eligibility checking. The discharge forms are returned to the hospital to be filed until the patient is discharged.

### Hospital Discharge Processing

Hospital discharge processing occurs after the patient has been discharged from hospital and the discharge form has been returned to OHIP by the hospital. Before returning the discharge form to OHIP the diagnostic information and surgical procedures are added to the form at the hospital. After receiving the form in the Hospital Claims Section of the Insurance Claims Branch the diagnostic information and surgical procedures are coded. Then the discharge summary is sent to Data Entry for input in the computer. Discharge processing involves checking and editing the information on the discharge forms as well as balancing information, for example, by checking the number of days in hospital against the difference between the admission and discharge dates.



## Hospital Discharge Reporting

The information compiled on a magnetic tape during the hospital discharge processing is run weekly and creates a file of valid discharges. In the final step of hospital claims processing the valid discharge file is used to update a hospital statistics file. Other information is extracted from the discharge file and is added to one of several subsidiary computer files for statistical purposes. The two major outputs of this processing are a list of cancer cases and a list of congenital anomaly cases.

## Claims Assessment Processing Subsystem

This subsystem is the major step in the claims processing cycle for services rendered by physicians, practitioners and laboratories. After completion of eligibility checking, the claims are subjected to various assessment rules such as checking for duplication (a participant can have only one appendectomy) and medical consistency (preventing charges for a male pregnancy). In addition, each valid claim has the appropriate fee schedule rate applied to determine the actual claim payment amount. After the checks have been made, the assessment processing generates two files, one of approved claims and one of rejected claims. Approved claims are used to update the claims reference file which contains the claims history of every participant. OHIP claims history data in 1978 required nearly 80 reels of magnetic tape. After the claims reference update, the approved claims pass through two other subsystems for cheque production and claims reporting.

Rejected claims are used to update the pending claims file. This file contains information on all rejected claims, thus requiring a claims clerk to enter corrections only of that information which was discovered to be in error. For all rejected claims, the associated claims history records from the claims reference file are copied onto a claims transcript file for printing. These claims transcripts are sent to the district offices with the list of rejects and with the appropriate resubmission forms. On a monthly basis, a claims reference computer output microfilm tape is produced and is sent to the Supply and Services Branch for the production of microfiche.

## Physician/Practitioner Profile Subsystem

The physician/practitioner profile system processes data from the following sources:

1. OHIP fee-for-service medical claims (4,000,000 claims per month).
2. Active treatment hospital claims (100,000 discharges per month).
3. Registry information retained on file (12,000 active physicians and practitioners in Ontario).

The computer system scans all services performed during the month and extracts data concerning physicians' and practitioners' practices from the claims submitted by other physicians and practitioners as well as their own claims. Once the information is structured according to service month, data about the physicians' and practitioners' own services, hospital claims, referrals made, services by other physicians and practitioners, and registry data are used to construct a series of profile reports. The reports are in a statistical form only. The statistical validity of the profile reports is affected by the omission of various sources of physician and practitioner income. For example, missing are payments to health centres, salary payments and additional income obtained from billing patients for the full fee schedule (OHIP pays 90 per cent of the amounts specified in the fee schedule).

The first stage of the profile subsystem processing occurs at the Leaside Data Centre, one of three government-owned computer centres located in Metropolitan Toronto. The first stage of processing, which includes extracting data from the claims reference file, the hospital statistics file and other practitioner related files, is very small in relation to the total processing involved in the subsystem. The output tapes are copied before being sent outside to an external service bureau for continued processing.

The second stage of processing occurs at a service bureau selected by the Ministry of Health. The copies of the profile computer system tapes are transferred to the service bureau by bonded courier. Every month the profile system is run at the service bureau, which performs most of the complicated detailed file manipulations and creates new computer files, including the combined detailed claims file, the dummy contract master, the detailed doctors' file, the detailed group file, the detailed hospital file, the physicians'/practitioners' summary master, the aggregate file, the three-month-old claim file, and the seven-month-old claim file. The tapes created by the monthly processing run are then returned to the Leaside Data Centre. There the data file system tapes run through further sorting and processing procedures and eventually a variety of profile

reports are produced. In addition, some profile reports are printed off-site at a firm called Offline Support Inc. These reports, along with magnetic tape files sent to Offline Support Inc., are returned to the Leaside Data Centre by courier.

## Claims Reporting Subsystem

The claims reporting subsystem uses as input three magnetic tapes produced by the claims assessment system, namely, the approved claims file, the rejected claims file, and the claims adjustment file. The processing in this subsystem is straightforward and results in the production of various system reports, such as the rejected claims report, the claims status reports, claims resubmission forms, and the claims adjustment reports.

The first three reports are returned to the nine district offices for use in handling claims inquiries and in reprocessing rejected claims. The last group of reports, the claims adjustment reports, are sent to the claims payment section of the Finance and Accounting Branch. In addition, bi-weekly and monthly claims status reports are produced and distributed to district offices and head office.

## Claims Payment and Accounting Processing Subsystem

The claims payment and accounting processing subsystem handles the payment and accounting of all medical claims within OHIP. For pay-subscriber claims, cheques are produced immediately upon processing. For pay-physician or pay-practitioner claims, the system accumulates the claims payment information for the physician or practitioner until the end of the month. At that time, a single cheque is generated for each physician or practitioner practice for the month, along with remittance advice showing all approved claims which are incorporated in the cheque amount and all disallowed claims. The subsystem also maintains accounting history files for both physicians and practitioners and for subscribers. The subsystem also generates a computer output microfilm tape of remittance advices which are then used to generate microfiche of all remittance advices.

## Information Flows Between Major OHIP Organizational Units

The following are the major information flows within the OHIP system:

1. enrolment information flow,
2. medical claims submission flow,
3. medical claims inquiry flow,
4. medical claims resubmission flow,
5. hospital claims submission flow,
6. practitioner registration flow,
7. microfilm and microfiche processing flow,
8. Leaside Data Centre flow,
9. practitioner profile information system flow.

Each of these is discussed in detail below, along with important points at which security exposure is possible. These points are called control points.

## Enrolment Information Flow

Residents of Ontario register with OHIP through the enrolment process (see Figure 4). The OHIP subscriber may register with OHIP either as a member of a group or through a pay-direct mode. A subscriber who enrolls as part of a group registers with OHIP through his or her employer. The pay-direct method is used by individuals or by small groups of employees (under 15 in number). While group subscribers pay through their employers, pay-direct members pay their premiums directly to OHIP. The enrolment process requires a subscriber to complete one or more forms, including, if necessary, such special forms as an application for premium assistance. Information from these forms is put onto a magnetic tape for entry to the OHIP computer system.

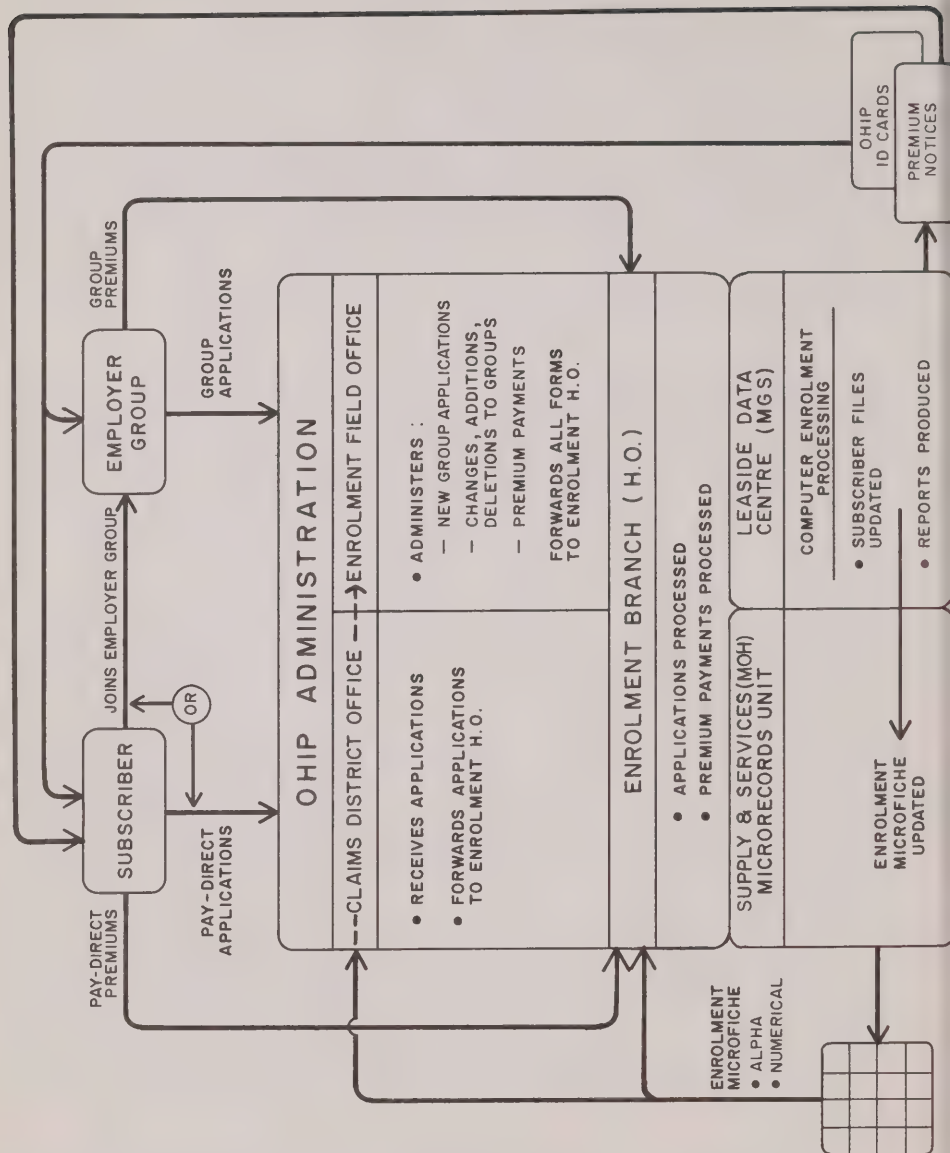
The computer system is used to maintain a master file of both group subscribers and pay-direct subscribers. On a routine basis, the subscriber master file is output on microfiche for distribution to the district offices and head office where they are used for handling inquiries. This latter microfiche process may be replaced by the newer method of allowing district offices direct on-line access to OHIP master files.

The study of the enrolment process identified 15 control points at which information was transferred from place to place. Of these 15 points, four were determined to be important control points, that is, those requiring awareness as to their potential for presenting a risk of breach or loss of security. The four important control points in the enrolment process are as follows:

1. Off-site data entry of enrolment transactions. This data entry involves the handling of personal information. Data processing service bureaus and Ministry of Health

# ENROLMENT (AND PREMIUM COLLECTION) FLOW

FIGURE 4





facilities, other than OHIP, are used. This point is important since there must be an assurance that there will be no off-site unauthorized duplication of magnetic tapes.

2. A municipal social assistance or welfare file is kept in an area known as the Special Services Unit. This information represents potential access to an organized file of municipal social assistance recipients in Ontario. The file contains personal non-medical data and information about an individual's situation as it relates to his or her receipt of social assistance.
3. A similar situation exists with respect to files which are maintained on persons receiving special temporary assistance. Personal and non-medical data are kept and there exists the possibility that a master list of recipients of temporary special assistance could be created.
4. Hospitals are notified concerning the eligibility of persons requesting special assistance with respect to their OHIP payment. Personal financial information as well as hospital admission information may be revealed in this process.

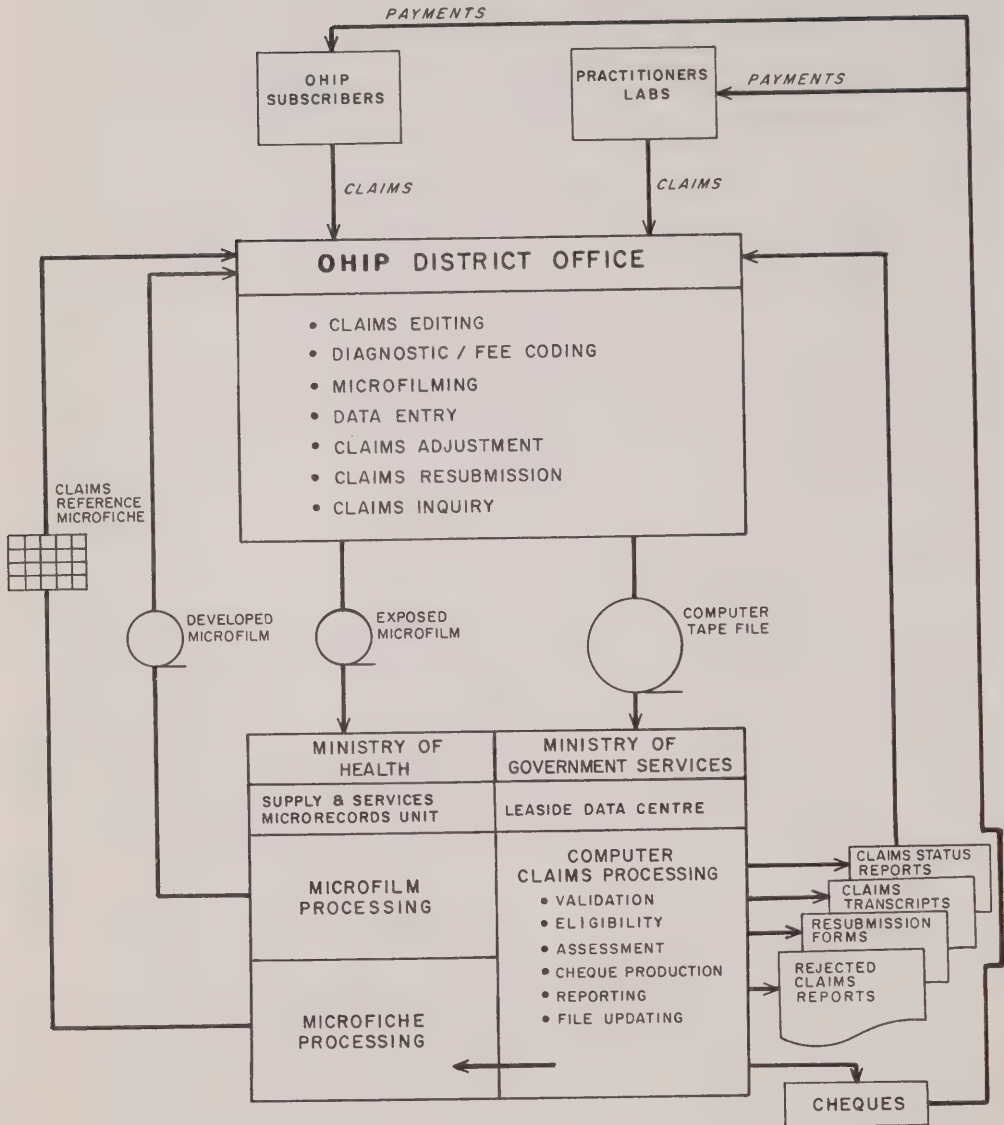
## Medical Claims Submission Flow

A claim may be submitted to OHIP by a physician, practitioner or subscriber. When a subscriber wants to make a claim for payment for medical services the claim may be submitted for payment to the physician or practitioner providing the services, if he or she is opted in, or to the subscriber himself or herself if the physician or practitioner is opted out of OHIP. This section deals with claims submitted on behalf of individuals. Claims submitted by hospitals will be dealt with later. Practitioners usually submit claims on behalf of the subscribers.

All medical claims are submitted to OHIP through one of the nine district offices (see Figure 5). The district office examines claims for missing information, codes the diagnostic and fee schedule information, microfilms the claim cards, and enters claim data onto magnetic tapes. Claims are handled by claims processing clerks in the district office and are eventually sent to the OHIP computer system for processing. Claims processing procedures in all district offices were changed after the successful completion of a pilot project in the Hamilton District Office in the early part of 1977. The new procedures reduce the operation costs, time and paper necessary to process

FIGURE 5

# MEDICAL CLAIMS FLOW



claims. In the first stage of processing, the information from the claims cards is entered by a keytape operator onto a video terminal connected to a mini-computer. The information is checked and edited and then placed on a disk pack. The data are then put onto a magnetic tape and run through a program which checks the data for errors. The resulting error-free tape is then sent to the Leaside Data Centre and processed in the same manner as the tapes from the other district offices. Some health-care groups use their own facilities or private service bureaus to prepare a magnetic tape containing the claims information which is then submitted to the OHIP district office for error checking.

Nineteen control points in the medical claims system processing procedure were identified by the study. Of these nineteen control points, nine points were thought to be important and two of these important ones were considered critical.

The important control points are listed in the following description:

1. The point at which medical claims are opened in the district office mailroom. Medical claims cards containing personal and medical information about individuals are batched by practitioner and collected together. There is the potential here to identify all the services provided by a practitioner.
2. A similar access problem exists at the point at which these cards are date-stamped and sorted.
3. A clerk adds the diagnostic and fee schedule codes to the medical claims cards. The claims preparation clerk may use microfiche records produced by the OHIP computer system which contain all patient information. These data are organized by OHIP number and are readily accessible. Personal data, medical data, and all claims data for people who have submitted a claim through OHIP within the last six months are included on the microfiche records. This was considered a critical control point.
4. When practitioners make use of service bureaus to prepare their claims, a potential for exposure exists. Individual claims records are put onto magnetic tape or punched cards for submission to the OHIP office. External computer service bureaus are retained for this purpose. This creates the possibility that someone could have access to these records during storage and processing, and, of course, puts OHIP information outside the control of the

physicians and OHIP itself. This was considered a critical control point.

5. If an external service bureau is used for the preparation of physical claims, the information must be transported from the computer service bureau to the district office. Couriers could gain access to these records during the time they are out of the direct control of OHIP or the physicians.
6. At the time medical claim tapes are filed at the district office there is the potential for the duplication of the tape utilizing nearby equipment.
7. At the time the medical claims cards are filed there is the potential for access to a large number of medical claims records in one location.
8. After all claims tapes have been prepared by a district office they are sealed in a sack and a courier picks them up, along with a bill of lading, for shipment to the Leaside Data Centre for computer processing. During the time the tapes are in the hands of the shipping organization there is the potential for overnight duplication of magnetic tapes at an off-site location.
9. At the receiving end, the courier sack is opened and checked against the bill of lading. This represents a security problem since there is the potential for failure to notice missing magnetic tapes through inadequate verification against the bill of lading.

## Medical Claims Inquiry Flow

A claims inquiry from a physician or practitioner is usually made when the physician or practitioner feels that he or she has been overpaid or underpaid on a specific claim. The inquiry is made in writing to the district office. The claims processing group at the district office rechecks the claim in question to see if an error was made. To accomplish this, the original claim card is retrieved from the files and a hard copy printout of the claims reference microfiche for the particular subscriber in question is requested from the microfilm area of the district office. If adjustments are required, an adjustment form is completed which is microfilmed and entered at the district office. Adjustments are then treated as new claims and follow a procedure identical to that of the medical claims submissions. The claims processing clerk records the resulting

action on the inquiry form and returns a copy to the requesting practitioner or physician.

The following important control points in this process were identified:

1. The requesting of hard copy of individual histories from claims reference files stored on microfiche represents a critical exposure requiring strict control since there may be unauthorized requests for claims histories. This was considered a critical control point.
2. When the information is retrieved a copy is made of the individual medical history from the claims reference records, the auditing of the requests and control of the retrieval of microfiche records are critical. This was considered a critical control point.
3. The matching of the microfiche medical history with the claims cards in response to an inquiry request represents a potential for exposure since there must be control over a person who receives or handles the total medical history of an individual. This was considered a critical control point.

## Medical Claims Resubmission Flow

After claims have been processed by the OHIP computer, various computer reports are returned to the district offices for inspection. These reports include a listing of all claims rejected by the system, transcripts for claims which have been rejected and claims status reports. Claims resubmission forms are included. When resubmission is necessary the district office pulls the original claims cards from the files and matches these with the computer reports before processing.

During the correction process, the claims clerks make adjustments directly on the resubmission forms under the data that are missing or in error. These resubmission documents then follow a data entry process similar to that described above and are then submitted to the OHIP computer system for reprocessing. The following important control points were identified:

1. There is potential for exposure at the OHIP office when the claims submission forms, transcripts and various reports are packaged and during the removal of documents and retrieval of cards using the rejected claims lists. The detailed claims histories of individuals are accessible by



district office staff, by couriers and by mail handling clerks. This was considered a critical control point.

2. When the processing of the document is complete, the claims transcripts must be destroyed. There is the possibility during this process that the transcripts may not actually be destroyed and that others could have access to them. This was considered a critical control point.

## Hospital Claims Submission Flow

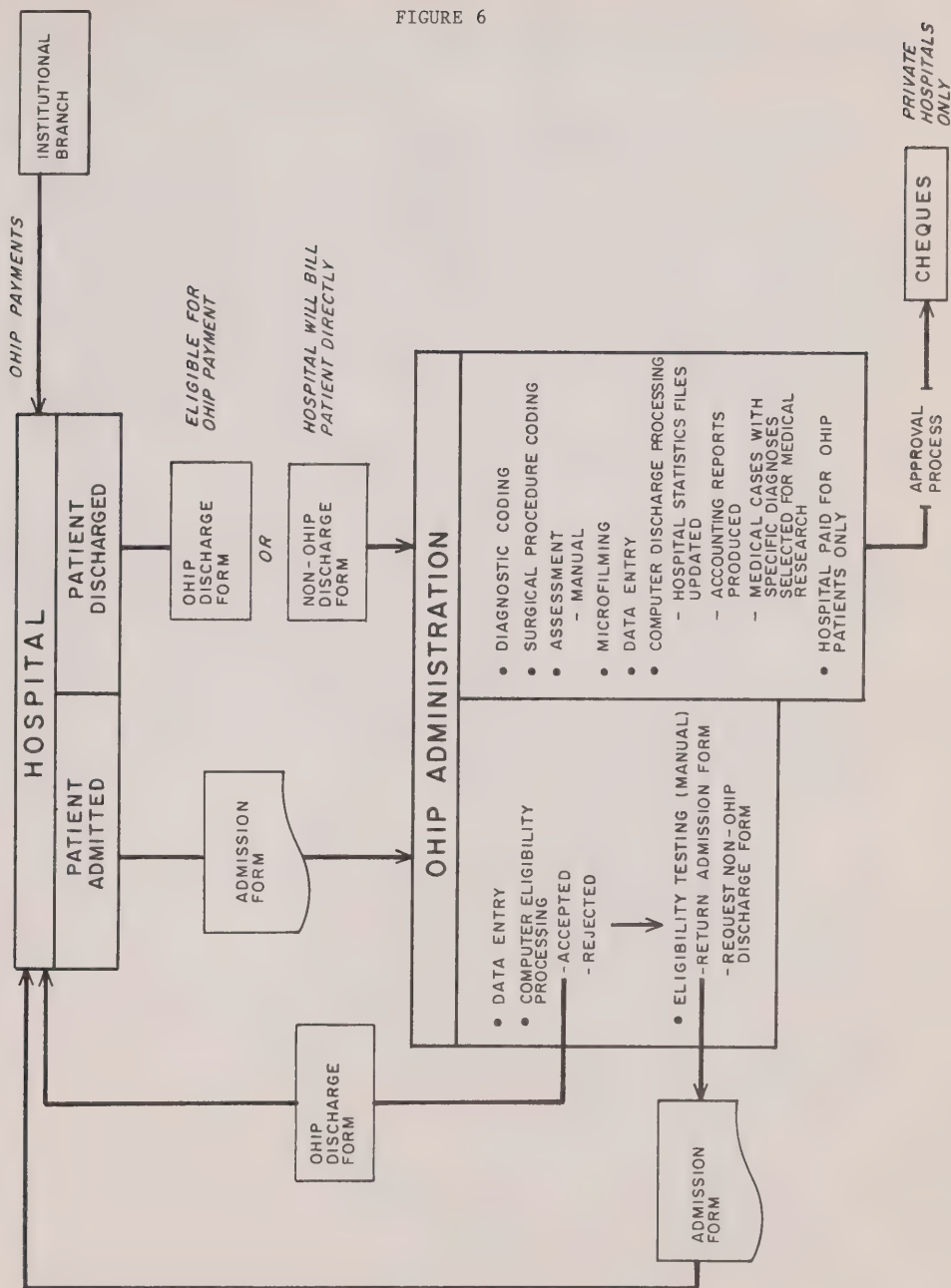
Several types of hospital claims are handled within the OHIP system. In-patient hospital claims from Ontario hospitals represent the bulk of these claims. Less frequently there are out-of-province or out-of-country claims, chronic care hospital claims, or private hospital claims. These less frequent types of claims are not dealt with further here. The hospital claims submission process occurs in two parts (see Figure 6). The first part of the claims process take place when the patient is admitted to the hospital. At this time, the hospital completes an admission report and sends it to OHIP. This information is keyed onto magnetic tape and entered into the OHIP computer system where the patient information is checked for eligibility under OHIP. For all eligible patients the OHIP system automatically generates a hospital discharge form. For rejected patients, a manual check of eligibility is performed. If the patient is deemed to be a valid OHIP subscriber by this manual process, a discharge form is prepared manually. A rejected admission, that is, an admission for a patient not eligible under OHIP, is returned to the hospital with a request that the hospital complete a non-OHIP discharge form when the patient is discharged. All the discharge forms are completed by the hospital at the time of patient discharge.

The second part of the claims submission process occurs when the patient is discharged from the hospital. At this time the proper OHIP discharge form is returned to OHIP. This form contains information concerning the procedures carried out in the hospital and the length of stay. OHIP codes the diagnostic and surgical procedures prior to input to its computer system. The forms are then microfilmed and sent to the Data Entry Section of the Systems Management and Co-ordination Branch (SMAC) of the Ministry of Health. Here the data are input into the hospital claims discharge system on the computer.

During our assessment of the study we observed that the handling of physiotherapy claims cards at the Hospital Claims Section of OHIP provides a point at which there is ease of

# HOSPITAL CLAIMS FLOW

FIGURE 6



access to information and potential for misuse. This was considered a critical control point.

## Practitioner Registration Flow

Physicians and practitioners must be registered with OHIP before claims can be submitted by them to OHIP. A physician may register as a sole practitioner or as a member of a group of physicians. He or she must also decide whether to opt in or opt out of OHIP. The computer system maintains a computer file of practitioner registry information and also periodically generates practitioner reference information on microfiche. No important control points within this process were identified.

## Microfilm and Microfiche Processing Flow

Microfilm and microfiche are both photographic methods of recording information in a high density form. Microfilm is ordinarily kept in a roll form either on reels or in cartridges, while microfiche is usually stored in flat form on pieces of film approximately 4" x 6" in size. Microfilm is generated when a source document is put under a camera and its image recorded on film. Microfiche, on the other hand, is generated from information stored on a magnetic tape using a special processing machine known as a COM (computer output microfilm) device. One microfiche can store the equivalent of 200 or more pages of computer printout.

The basic processes involved in handling both microfilm and microfiche include developing, quality control, duplication, inspection, packaging, and distribution. The master copy of the microfilm or microfiche is retained in the Microrecords Unit of the Ministry of Health for one month and is then sent out for archival storage. Microfilm and microfiche copies are distributed according to the needs of the district offices and head office within the OHIP system (see Figures 7 and 8). Six important control points were identified during the study, four of which were considered critical.

1. Data prepared for microfiche output are received on magnetic tapes and a master film is produced. During the process of handling the tapes and the production of the film there is potential for the loss and misplacing of the tape to be output on microfiche.
2. The printing and processing of the duplicate copies of the master microfiche provide an opportunity for unauthorized

# MICROFILM PROCESSING

FIGURE 7

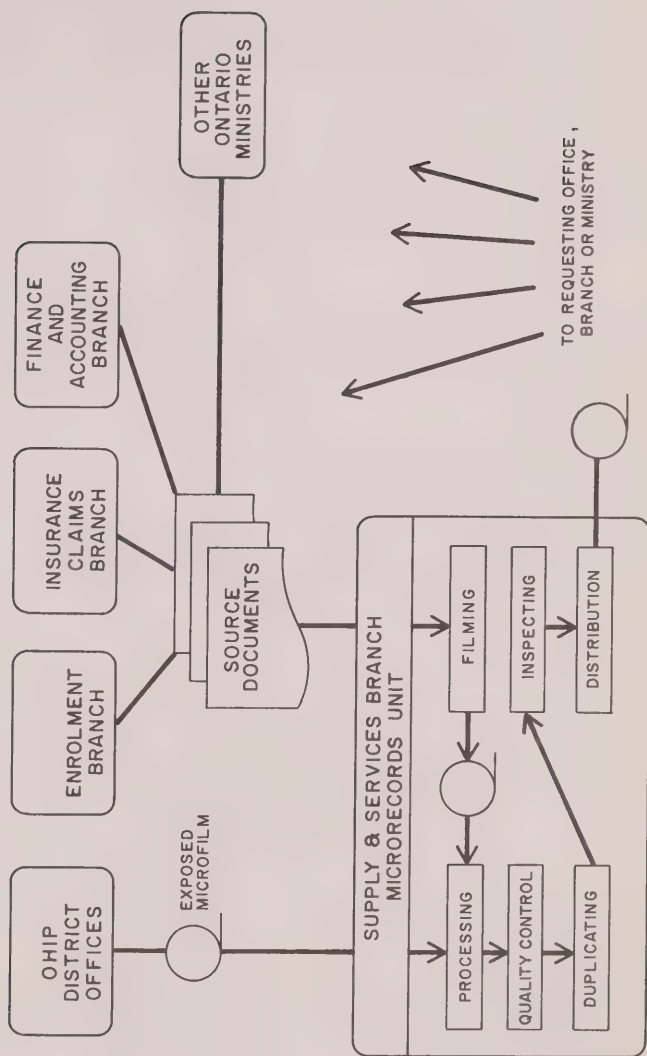
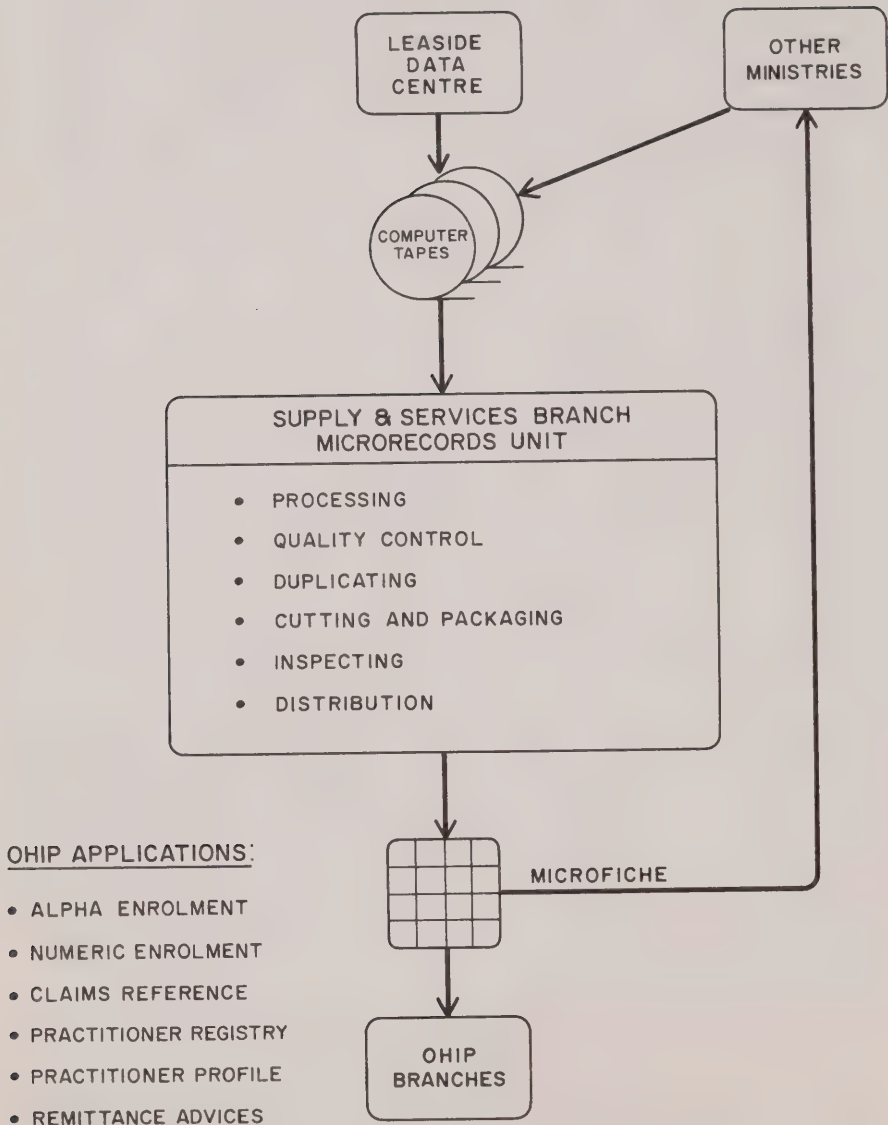


FIGURE 8

## MICROFICHE PRODUCTION





production of masses of personal medical and financial OHIP data. This was considered a critical control point.

3. Once produced, the microfiche copies must be cut, collated, and packaged. The microfiche at this point is in a form readily usable, transportable and compact. The control of distribution is important. This was considered a critical control point.
4. After its production, the microfiche is quality controlled to make sure it is of the proper thickness. The microfiche could be subjected to unauthorized rejection or abuse during this period.
5. Once the microfiche is measured, it undergoes a visual inspection of the microfiche. The opportunity exists here to select and retain microfiche for unauthorized use. This was considered a critical control point.
6. After they have been completely checked, the microfiche copies are distributed to the filing area for retention of a copy, to users, and to the Microfiche Records Centre. During distribution, access to the data can be obtained and there exists the possibility that the data may be misused. This was considered a critical control point.

## The Leaside Data Centre Flow

The Leaside Data Centre, located at 15 Overlea Boulevard in the Borough of East York, is run by the Ministry of Government Services on a service-bureau basis for the Ministry of Health. The major functions of the Leaside Data Centre, which operates like any other computer data centre or service bureau, include the following:

1. The operation and maintenance of the computer and related devices.
2. The storage of computer files in various forms (magnetic tape, disk, etc.).
3. The receipt of computer input files from outside areas.
4. The preparation and scheduling of computer processing runs.
5. The actual processing of OHIP information on the computer.

6. The production, sorting and distribution of computer output.
7. The transportation of computer information to outside service bureaus and to users.

During the investigation six important control points were identified, four of which were considered critical.

1. The computer transaction files on magnetic tape or on punched cards and the registration and verification of the actual media received, if not carefully controlled, may be lost or misused.
2. During computer processing of data, there is the potential for unauthorized copying and altering of OHIP computer records. This was considered a critical control point.
3. OHIP utilizes off-site storage and cycling of computer files because of the large processing load. During this time, control of OHIP files passes out of the direct control of the Ontario government. This provides an opportunity for unauthorized duplication or use of the data. This was considered a critical control point.
4. In the processing of profile information, magnetic tapes are released to an outside service bureau, which also stores copies of the tapes. During this period of time detailed OHIP files are beyond direct government control. A potential for the abuse of this information exists. This was considered a critical control point.
5. Reports are produced as part of the physician-profile system and are sent to an external service bureau which prints out the contents of magnetic tapes. There is the opportunity for loss or misuse of these reports or of the tapes.
6. Once reports are produced for distribution, they must be sorted and prepared for pick-up or distribution and stored temporarily until they are picked up. These reports could be lost or examined by unauthorized personnel. This was considered a critical control point.

## The Practitioner Profile Flow

The practitioner-profile subsystem uses various OHIP files to produce aggregate statistics on physician and practitioner

activity over given periods of time. These profiles are made available to physicians or practitioners on request to the Professional Services Monitoring Branch.

The following important control points in this system were identified:

1. There is the opportunity for unauthorized requests to be submitted and processed along with genuine requests. Although there is a verification process for request authorizations, it is possible for unauthorized requests to be submitted and not detected.
2. Computer terminals may be used to submit profile requests through the Ministry of Health. The potential exists for access through external service bureaus or others outside government jurisdiction if there is not adequate control.
3. As part of the profile request, a claims transcript hard copy is produced from microfiche. This provides an opportunity for an unauthorized person to secure a detailed medical history of an individual through a failure in the control process. This was considered a critical control point.
4. Once a profile has been requested, it may be retained while awaiting release. With authorization, the report may be released to the Professional Services Monitoring Branch. This provides a potential for abuse and detailed analysis by unauthorized persons.
5. The copies of the profiles are filed and used internally within the Professional Services Monitoring Branch. Since the information is sensitive, control of access is important. This was considered a critical control point.

## Study Findings and Observations

The following general findings and observations resulted from control-point testing in the following areas:

1. District Offices, the Insurance Claims Branch,
2. Microrecords Unit, the Supply and Services Branch,
3. Leaside Data Centre, Ministry of Government Services, and
4. the Health Insurance Division.

The testing was performed on 18 critical control points of highest concern identified in these areas. The comments below are

classified as "critical" (i.e. requires immediate attention), or "non-critical" (i.e. merits comments), and all comments relate to the situation observed at the time of the study.

## District Offices

### A. Critical

- A.1 The disposal of confidential material at the district offices is a problem in some of the offices visited. Bins (boxes, barrels) used to dispose of the claims cards, claims reference transcripts, hard copy reproductions of the claims reference microfiche, etc., are left in the claims processing areas until full, a process which often takes several days. Several of the offices have addressed this problem by emptying the containers daily and locking up the contents for shredding or destruction on the next working day.
- A.2 The storage of microfiche in district offices is a general problem. While most offices lock up the current versions of the microfiche every night, in several cases the old microfiche was left in unlocked drawers or on open shelves. In the case of the claims reference microfiche the old data are just as confidential as the current data.
- A.3 There is a control weakness in the disposal of old microfiche. Most district offices return their old microfiche (according to the retention schedule) to the Microrecords Unit at 15 Overlea Boulevard for destruction. The district office records the information identifying the microfiche destroyed on the back of the retention schedule. The microfiche are bundled, boxed and shipped to the Microrecords Unit. However, the Microrecords Unit simply stockpiles the old microfiche, and does not record the receipt of the microfiche for destruction. There is a need for a control at the receiving end of this destruction process.

### B. Non-critical

- B.1 Throughout the study, there was observed a growing awareness in the district offices about security. This obviously reflects a changing attitude on the part of the Ministry to provide more control over the

confidentiality of health records. This change has been evidenced by the issuing of several memoranda on confidentiality, and the appearance of locked cabinets and locking bars on office equipment.

- B.2 The need for a hard copy of the claims reference information on microfiche is reduced in offices where accessibility to the microfiche is more prevalent. While providing access to microfiche may reduce paper, easy access implies more copies of microfiche and more readers, a much more critical hazard.
- B.3 In general, all offices feel that the claims information must be readily available to all staff in order to effectively process the volumes currently received. The oath of office and secrecy signed by all Government employees provides a measure of control over confidentiality.
- B.4 The new procedures first introduced with the Hamilton pilot data entry project appear to have several benefits including higher employee morale and fewer claim rejections. A more important benefit will be the reduced paper requirement due to the input of claims information on magnetic media. However, the new system introduces a third party to the process. Besides the physician or practitioner and OHIP, there will now be a service bureau acting on behalf of the practitioner. The Ministry must establish firm policies and guidelines regarding the use of these service bureaus and the access to confidential health information which they will have.

## Microrecords Unit

### C. Critical

- C.1 As mentioned in A.3 above, there is no control over the receipt of old microfiche for destruction. The information should be logged upon receipt and periodic audits performed to ensure that the retention schedules are being followed and that the microfiche are eventually destroyed.
- C.2 The distribution lists for microfiche applications are too informal. They are handwritten, unsigned and undated. In addition, correspondence from the Health Insurance Branch kept by the Microrecords Unit did not



authorize duplication volumes or distribution at the time of the study.

- C.3 There is weak control over the microfiche duplication process. The permanent copy counters in the duplicators are not being used as a control over microfiche production as they should be. The start and end readings should be recorded daily, and the production volumes justified to match the daily readings.

D. Non-critical

- D.1 Rejected microfiche from the inspection process are placed in containers within the COM area. The containers, however, as in some of the district offices, are not emptied until they become full. However, the entire COM area is locked at all times, making this issue less critical.
- D.2 Until August, 1978, authorized signatures were not checked before making "printouts" from microfiche. In July, 1978, the procedure for requesting and producing printouts was modified. With the new procedure, which includes a new Printout Request Form with authorizing signature box, the printout requests are checked for proper authorization before the hard copy printouts are made. This new procedure will ensure a proper control over printout requests.
- D.3 The procedures for handling the master copies of all microfiche are adequate and provide effective control. The use of retention schedules, and the government's Records Centre in Mississauga provide the control.

Leaside Data Centre (Systems Management and Co-ordination Branch, or SMAC)

E. Critical

- E.1 There were no areas in which control procedures could be considered critical.

F. Non-critical

- F.1 Physical access control procedures to the data centre are effective. The two-level access (cypher lock,

badge) provides protection. However, the issuance of lock combinations and badges should be reviewed so that cleaning staff will be required to be escorted into the data centre.

F.2 OHIP processing follows the same pattern daily. Any attempt to copy a critical file or produce an extra report would affect the processing time and would likely be noticed immediately by either Operations or Client Services Staff.

F.3 Terminal access to OHIP files is not widespread. The bulk of OHIP files are on magnetic tape because of the size of the file (the claims reference file comprises 79 reels). Tape files cannot be read from the remote terminals in use within SMAC without first authorizing a computer run to copy them to disk. Moreover, several codes must be known in order even to sign onto the system. These are the following:

- LOGON identification code,
- password,
- access code.

Furthermore, some files are password protected (see F.4 below).

F.4 File password protection is limited in use. The Leaside Data Centre has the capability of providing password protection to files but the direction and onus must come from the users, the Health Insurance Division and SMAC. There are currently very few files with passwords.

F.5 File storage is adequate from the point of view of control. File retention is on a scheduled basis with the following three levels of protection:

- computer room tape library,
- locked vaults at 15 Overlea Boulevard,
- off-site storage at Data Security Limited.

F.6 Off-site processing at the service bureau under contract seems to be well-controlled, but it appears that no one from the Ministry has physically inspected the service bureau as far as security is concerned. The particular bureau in use at the time of the study is very security conscious. Tape pick-up and delivery is escorted at both ends, and picking-up lists are authorized at both ends.

- F.7 Controls over output distribution are adequate. Internal Ministry outputs are placed in lockable boxes in the client services area. The users are issued keys, and have the option whether or not to keep their output secure from other users.

## Health Insurance Division

### G. Critical

- G.1 The distribution aspects of the critical microfiche applications, that is, claims reference, alpha enrolment and numeric enrolment, need immediate review. In general, very few District Office directors knew how many copies of the microfiche they received, why they needed them, how long they kept them, and what they did with the old versions when they were updated. In one case, a District Office received three copies of the alpha enrolment fiche. One was used in the office and two copies were filed in a vault and never used. In the case of the Professional Services Monitoring Branch, the one copy of the claims reference file received is passed on to the Medical Review Committee of The College of Physicians and Surgeons of Ontario.

The review of the OHIP system was extensive, but not exhaustive. Efforts were concentrated on the segments of OHIP which result in 90 per cent of the day-to-day activity. As a result, sections such as subrogation and out-of-province claims received little attention, whereas the basic functions of enrolment, claims processing and file processing for basic claims were emphasized. The Subrogation Branch's operations are explained elsewhere in this report.

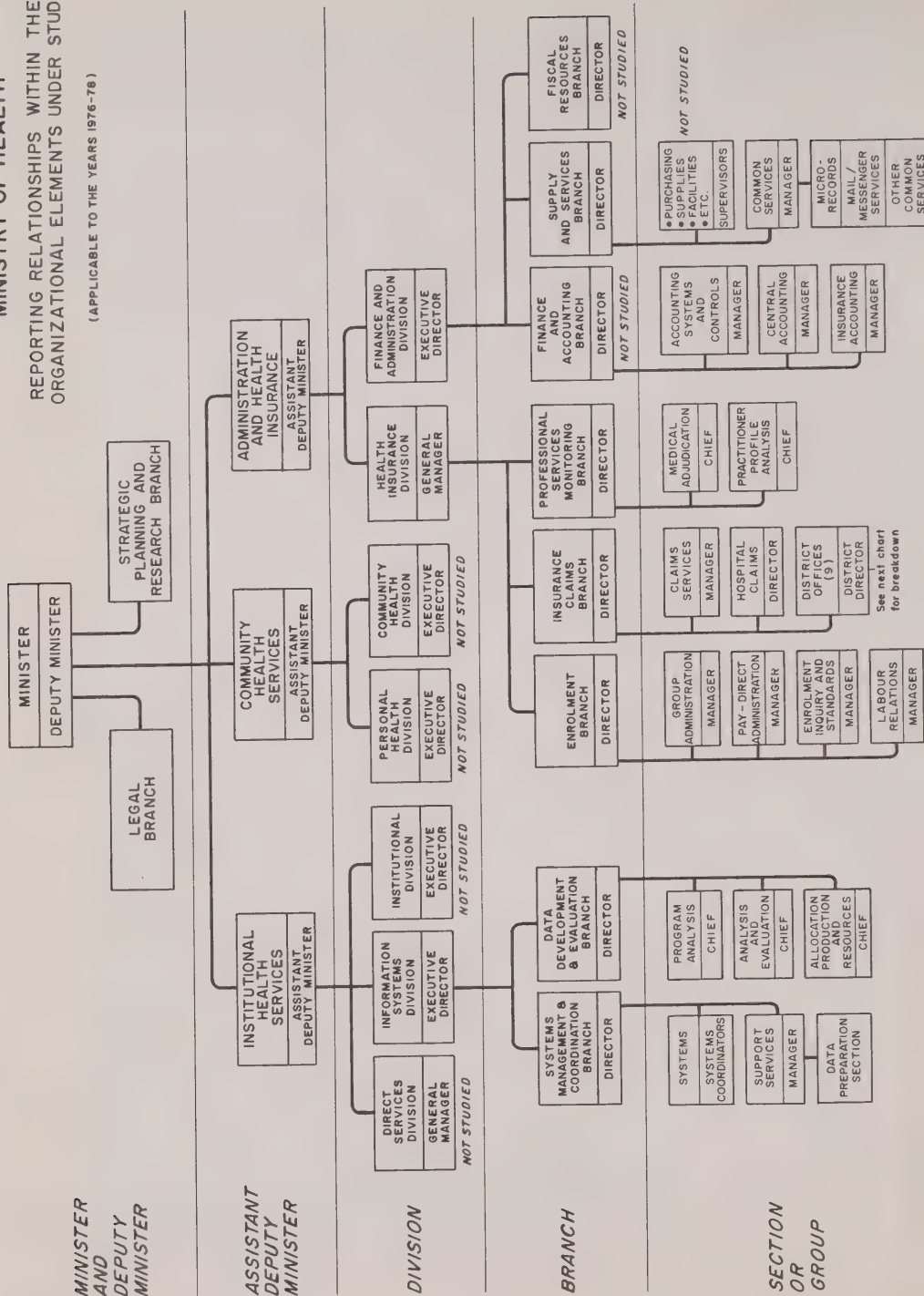
Since 1978, when the study was completed, several changes in the processing of information and security measures have taken place. As of October, 1978, hospital claims processing is done through the district offices rather than directly through a central office. The admissions report (106A) is sent by the hospital to the district office which then forwards a tape containing the information to the central hospital claims section which checks the eligibility of the patients. Rejected admissions are sent to the district office. The discharge reports (106D) are generated by the hospital claims section and returned to the hospital. After the patient is discharged the 106D is returned to the district office where it is merged with the 106A file. The magnetic tape containing the merged 106A and 106D files is then combined with the computer file containing

information submitted by the hospital to the Hospital Medical Records Institute to form the Ontario In-patient file. This file, maintained by the Ministry of Health, is used to prepare the same type of reports as those derived from the 106D file discussed above.

In 1979, a security manual was prepared and issued to all OHIP offices. The manual includes instructions for the storage and destruction of all confidential information. Furthermore, the numbers of copies of the claims reference and enrolment microfiche are declining. In August, 1980, all computer production files, including the claims reference file, became password protected.

## REPORTING RELATIONSHIPS WITHIN THE ORGANIZATIONAL ELEMENTS UNDER STUDY

(APPLICABLE TO THE YEARS 1976-78)





## Computer-Supported Systems in Health: The Threat to Privacy

This section of the report consists of a discussion of the relationship between computer technology and the confidentiality of health records and the effect of the former on the latter. Because the subject is necessarily technical, a somewhat foreign terminology will be apparent. Indeed, so specialized is the subject and the language of the subject that it could not have been studied and this section could not have been written, without the advice, guidance, and instruction, both oral and written, of an expert in computer science. My consultant has been H. Dominic Covey, assistant professor of Computer Science, University of Toronto, and director of Cardiovascular Computing, Toronto General Hospital, whose contribution I have acknowledged in the early pages of this report. For the assistance of the non-specialist reader a partial glossary of terms may be found at the end of the section.

The public is becoming increasingly aware that information shared with the health-care system will often ultimately find its way into a computer system for any of a variety of purposes. Some information gathered during the investigation and treatment process is needed, for example, to document the patient's contact with the health-care system so that the hospital or physician can be remunerated for services rendered. Frequently the institutions themselves register patients on various registries for the purpose of efficient administration and proper use of resources. A good example of this is the registration of patients on an admitting system or a patient registration system at a hospital. A given patient's information may be recorded in any number of other data bases, such as those created for research purposes, or as required by law as in the case of venereal disease registries. Finally, as computer technology becomes cheaper than paper and manual systems, records will increasingly be stored on the disks and tapes of computer systems simply because it is cheaper for them to be there.

As their information finds itself more frequently on computer systems, patients are becoming aware that a threat to their privacy may be involved, since they assume that the information they shared with the health-care system is confidential and only for restricted use in the service of their health care.

The public sees the shared information as being "exposed", that is, susceptible to misuse, in a variety of ways. For example, unauthorized persons may read the information, link it to other information, share it with unauthorized third parties, use it to undermine a person's insurance status, exploit it for purposes of personal embarrassment, and so forth.

All of us are aware of the existence of computer fraud and of the misuse of even health information for such purposes as political embarrassment. The awareness of the fact that computer systems are less than perfectly secure is growing, mostly through media treatment of crime relating to other computer-based systems such as credit systems. Concern about the privacy of information is stimulated partly through knowledge of legislative activities in the United States with respect to privacy and the freedom of information. Now and then low level uneasiness turns into momentary disturbance because of particularly distressing revelations such as the purported viewing of the venereal disease file, an event known as the "VD fun run".

Although the public is aware of the issues and can imagine potential threats to their privacy from illicit access to computer-stored information, the fears are not well based and are of a general nature only since the technical aspects of computer systems security are not well known. The case can also be made that since, at the present time, the public is not aware of what information is kept, the degree of exposure possible is also not fully appreciated. Although it can be said that there is ignorance of the degree of exposure of privacy, that anecdotal threats raise what may be irrational fears, and that awareness of the issue of privacy, its value, and the threats to it are growing, there exist neither legislation nor guidelines to effect a balance between the desire for individual privacy and the needs of organizations for information.

Almost all agencies which utilize computer systems to store and process health information in any form are conscious of this growth in public awareness and are recognizing the need to develop a sense of responsibility to protect the information with which they are entrusted from disclosure or destruction lest they discredit themselves in the public eye. Nevertheless, few agencies have any idea of the level of sensitivity that each data item has as perceived by the individual who shared it, have a quantitative and demonstrable justification for their collection of each data item, or have a genuine idea of the potential threats which might exist to the systems they use to store this data. Among those agencies that know they have a "need to know", few know to what level they should raise their security protection measures and at what point the implied costs would be

excessive relative to the sensitivity of the information and the potential threat from intruders.

Many persons have expressed their views and concerns on this issue of the cost of security measures. At our policy hearings, David Harry, director of the Management Systems Branch of the Ministry of Health, put it this way:

You cannot make a computer impregnable. Basically the level at which you want to make it secure is a pragmatic decision as an organization you have to make, based on things like sensitivity of data, the amount of time and resources that you can put into making it secure.

David Milne, marketing manager of the Data Processing Division of IBM Canada Ltd., expressed this view:

[Systems] have to be economical. If the cost of the security precaution is ten times the benefit of using the system, it's not going to sell.

The brief of Prescription Services Inc. (Green Shield Prepaid Services Inc.) contains these submissions:

We feel that there must be an obvious balance between an adequate system of controls and misuse. There is very little point, in our view, in establishing a very high cost security system (which is capable of being invaded) to protect against misuse or abuse which may not exist....It is recommended that any security safeguards against programmer and operator invasion of the computer be realistic in relation to the degree of risk, the seriousness of disclosures and the cost of implementation.

The individual placed in the position of having to provide information is in an even more difficult predicament. He or she does not know what part of the information that he or she is requested to give is truly essential (or just demanded for convenience), how much of that information is stored, where and for how long it is stored, how well it is protected from destruction and disclosure, what is the real potential for unwarranted access, and what, realistically, he or she can do about the situation, if the answers to these questions were known.

If no one ever committed computer fraud, if something like the "VD fun run" could have been immediately dismissed as ridiculous and impossible, if the police were never known to seek health data for any reason, if computer input media such as cards were never found in garbage piles or blowing about the street, if no one collected more information than absolutely needed, and if the computer's ability to replicate and circulate data in huge volumes at extremely high density were not a physical reality, there would be no need for the individual to worry or for the agency to be concerned. In fact, although we have been lucky so far, serious questions have been raised, real dangers have been uncovered, and potential for misuse does exist. It is time to review the facts and formulate both philosophy and practical guidelines in an effort to reconcile the two frequently competing interests of the protection of the individual's privacy and the needs of organizations for information. The individual needs facts. What information does a given agency need? How secure can one expect those systems that hold the information reasonably be expected to be? How exposed is the information and consequently the individual's privacy? The agency needing data requires other facts. What is the perceived sensitivity of the individual's information? What rights does the individual have? What threats exist to the agency's computer systems? When is the agency liable? What is the minimum standard against which security will be measured?

The purpose of this section of the report is to address general and particular problems, to view these problems from the perspective of both the data-gathering agency and the individual, and to provide recommendations in order that the valid needs of each are effectively served.

Computer security is that subject which deals with methods that can be used to prevent unwarranted access to data stored on a computer system, unwanted destruction of that data or of the computer system itself, and unauthorized changes or additions to data or to the programs which process data. Computer security involves itself both with physical access, that is, access to the computer and to the storage media, and with what is called "logical" access, that is, the use of the computer or its programs to reveal, modify or add data illicitly. Later the various methods that can be utilized to provide a secure computer system will be discussed.

The first question to be asked is why we are concerned about computers. Ultimately, the only reason for addressing the problems that computers create is that computers bring into stark relief the problems faced in any records system. It just happens that the very efficiency and nature of computer systems



makes these problems more evident. In fact, if a computer system is properly used and properly protected it provides a previously unattainable level of control and of monitoring the access to information compared with any paper record-keeping system.

Despite the capabilities that computer systems provide in controlling access to data, fears relating to computers arise out of various considerations. First, it appears to the public, and it is probably a valid observation, that the establishment of new data bases and of systems for collecting the data to put in them, is extremely easy. The constantly decreasing cost of computer technology, the availability of reasonable data base systems programs, the availability of affordable computer-compatible input media, and the potential for remote access to computer systems which may be part of widely distributed networks, all make it possible to collect data now, where it was very difficult or impossibly expensive to collect data in the past. The power of individuals or organizations to establish such systems seems to be completely uncontrollable and many feel that members of the public are not in a position either to determine which data must be shared or how well they are to be protected.

Second, the very density of data, that is the amount of data that can be stored in a relatively small physical space, is a problem since an intruder can carry off sometimes as many as tens of thousands of records on a single disk pack, perhaps weighing ten pounds. This ability to remove masses of data permits an intruder to be non-selective. If the record or records of interest are known to exist among these thousands, then the data storage medium (such as a disk or a high density tape) can be stolen and placed on another computer system and perused when it is convenient and safe to do so. This non-selective access to large numbers of records was impossible when all records were kept on paper, given the size of a single patient chart.

Third, computers also provide for the possibility of "invisible theft", that is the stealing of data without actually removing anything physical, such as a disk or tape. This can be accomplished by obtaining access to data through a CRT (video) terminal screen, or by transmitting data to a remote and possibly unknown computer terminal. Of course it is also possible to copy data stored on disks and tapes onto the intruder's own disk pack and to walk off undetected. Any of these modes of access can be accomplished without altering the source data. It is true that proper computer security system safeguards can be used to prevent such access, at least to some extent. Without proper safeguards, no trace whatever need be left of the



transaction. Nor is access to data already stored in a computer the only danger. A similar case can be made for such items as data input forms, cards or other input media which may, for example, be scheduled for destruction, but which can be taken without the knowledge of the guardian of the data. Examples of this problem were the finding of pathology reports belonging to The Wellesley Hospital blowing about Toronto streets, as described in the chapter on Hospitals, and the discovery that the Ontario Medical Association received OHIP cards found by accident, as described in the Association's brief to the Commission on Freedom of Information and Individual Privacy:

A package of discarded OHIP claim cards, apparently en route to being recycled, was intercepted and delivered to the O.M.A. office. The cards, containing the names and addresses of patients and their medical diagnoses, the names and addresses of practitioners who treated them, were shipped from the OHIP office without being mutilated in any way. These cards were turned over to the Minister of Health with the suggestion that he order an immediate halt to the shipping of un mutilated claim cards from OHIP offices.

Finally, the ability to produce large numbers of copies of data very quickly on high speed line printers or on computer output microfilm (COM) devices, makes getting a "silent" copy of data items far easier than it was ever possible with paper records. The utilization of computer output microfilm records (claims reference file microfiche) in the OHIP system provides a potential for breach of security simply because so much data is provided. It is cheaper to be non-selective with such massive output than to be selective, with the consequence that any collection of output contains far more information that can ever be utilized by the person to whom the output was provided.

Fourth, there is the potential for "invisible" modification, deletion or addition of data. The ability to write over magnetically stored data without leaving a trace makes this possible. Such alterations were difficult to accomplish in a paper record since erasures or insertions could be seen. Without proper computer systems security measures, alterations of that sort can be undetectable. If an intruder decided to so alter data, it could cause embarrassment to a patient, cover up evidence which might be used in a legal action, or establish a record to justify remuneration for non-delivered services. Changes to data can also be accomplished through simple error,

such as the accidental modification of the wrong patient's record or the adding of one patient's information to another patient's file. This type of error of misidentification of the patient is the primary one at which universal health identification schemes are directed. Again it must be recognized that all of these misadventures are possible with a paper record system, but they are potentially more problematic and more easily lost track of in a computer system.

Fifth, there is also the potential of utilizing the computer system to collate data which were never intended to be brought together. For example, data base software technology can link together different kinds of records on one computer system, or link together data sets on different computer systems, such as Workmen's Compensation Board and Ontario Health Insurance Plan records.

The discussion that follows took place at our policy hearings and is instructive. Dr. Allan Dyer is the assistant deputy minister, Institutional Health Services, John A. Sarjeant is the executive director of the Information Systems Division and Alan Burrows is the acting executive co-ordinator of the Drug Benefits Branch of the Ministry of Health.

MR. SARJEANT: Mister Commissioner, the first issue that we would like to discuss with you is the one of the unique personal identifier. As you know, the use of a unique number for every citizen would allow us to do a lot with our files that we don't now do, that become more complicated. So if everyone were to use an individual number, such as the social insurance number, which would seem to be the best choice for technical reasons, we would have a greater facility to collect information pertaining to health services rendered to any individual.

. . . . .

I think that the advantages are still inherently present in having a system which would allow us to link the, put together the patterns of individual utilization of the individual patients.

. . . . .

For research purposes, I might add in passing, perhaps that rather more detailed medical record obtainable through HMRI called inpatient activities, inpatient conditions, provides a facility for research in those conditions that are more serious....

The kind of things that we have thought were attractive over the years in having this ability to link, would be perhaps to link it with occupational information, occupational health is a matter of increasing concern, and we have pictured the facility of being able to link occupational records or environmental hazards with use of the health care system.

. . . . .

The drawback, of course, of having a unique numbering system is that it would pose a security threat....In my view, there is extreme difficulty in a large system like ours of extracting the kinds of information that an intruder might be interested in. It could be done, nonetheless, if one were a dedicated intruder, as I have said in this paper, and the very existence of the ability to link these things together raises the attractiveness, presumably, to somebody who wanted to obtain unauthorized access. So we would acknowledge that there is a threat to the...a threat that we don't now have would exist if we went to the unique number.

. . . . .

MR. COMMISSIONER: There are many systems which can't be linked now, except with a great deal of effort and money, and which would be much easier to link with a unique identifier. So if you don't have all of that information within the drug plan, and you don't have all that information within the occupational health area, and you don't have all that information within the OHIP claims system, when you put them all together you may have a lot more information.

Isn't that the argument for the unique identifier?

DR. DYER: Yes, absolutely.

. . . . .

MR. BURROWS: Firstly, there is this huge amount of data that is available, and there are indications both from within government and certainly we have had approaches from without, to utilize this information in any number of ways. But quite frankly, at this point in time we don't, the program is new enough and the resources have been limited to a degree where we haven't utilized that data perhaps to its fullest potential....

The professional aspects related to pharmacy are still aligned with a group called Drugs and Therapeutics. The program management of Drug Benefit is now aligned with the OHIP group. So that this other unit which is concerned with therapeutic needs of the population of Ontario, and would like to do some investigative work using our data, quite frankly doesn't have immediate access to it, and we have been examining with them...and as a matter of fact, I received a memo today suggesting that it would be appropriate to set up a meeting in the near future...to discuss the types of data that they feel they would need.

Of course, before any concept of sharing were to go forth, the question of confidentiality would have to be answered.

Data can be transferred from computer to computer or from file to file on a given computer. In banking systems thieves have effected the transfer of funds by debiting (even by a small fraction of a cent) client accounts and crediting by the same amount an account created by the thief. The transfer of data or funds can be accomplished either through direct access to the computer system or through special programs, known as Trojan horse programs, previously hidden in other computer programs and activated when the illicit transfer is desired. If an entire file can be copied onto a disk or tape, the disk or tape can be taken to another computer system and used.

It is also possible for paper systems to be subject to similar abuses. The fact that there are identification schemes common to multiple systems, that magnetic records can be over-written without a trace being left, and that non-selective access to masses of data is possible simply makes it easier to carry out such an adventure on a computer system. One of the requirements for the protection of individual privacy is that separately collected data sets should be kept separate and protected from linkage. Problems can also occur when a permitted linkage is undertaken, but, because of misidentification, an improper linkage occurs. For example, if two different persons are mistakenly thought to have the same unique identification number, the result will be that their records can be inter-digitated, perhaps embarrassing one or the other of them.

Finally, there is the problem of the number of people who handle or have access to data because of storage in a computer system. Data entry clerks, programmers, and even repair personnel can have easy access to the information either because they handle it or because they have access to terminals which they can use to peruse it. This type of problem was made public by the allegations that service personnel had gained access to the Ministry of Health venereal disease file. Although that access proved to be unlikely, it was in fact possible, and only after the revelation were proper security methods (installation of passwords) enforced to prevent access of that kind. In this connection, Mr. Covvey's brief makes the following helpful points:

It is quite easy for any person to enter virtually any computer area in one of our large hospitals, to destroy the equipment or computer media, or to simply walk off with backup tapes or even the disk packs currently on-line. Good sources of large amounts of...information are radiology patient registration systems and systems supporting an admitting department. It is virtually certain that the data on the media will not be encrypted and that it can be read on virtually any other computer system with compatible media. It is likely to also be true that backups are kept in the same area as the computer system so that deliberate destruction of the computer area results in complete destruction of all data files. Many database systems have no transaction log or audit trail facility with the result that destruction of the database can be



catastrophic and unauthorized perusal of files can go undetected.

Most minicomputer systems established for clinical research purposes are kept in unlocked areas and the comments made above apply equally well to research facilities. Many such systems are established with only the most elemental forms of systems software security such as password access control. Rarely is the data encrypted and most often access to the database is possible through unlogged direct interactions with the operating system. Rarely do such systems have adequate fire extinguishing facilities.

Sometimes terminals, records, and computers can even be subject to access by the public, when they are not adequately protected, a problem pointed out in the discussion of the OHIP system. Remote access terminals in OHIP district offices (allowing on-line system access), remote access to Ministry of Government Services computers from hospital terminals, or access from many terminals within the Ministry of Health itself means that it is difficult to keep systems "under one's nose", because not all accesses result in a physical encounter with at least one human being. This is one respect in which paper records systems were usually more controllable. I return to the discussion with members of the Ministry of Health at our policy hearings:

MR. HARRY: ...under a controlled environment we have been testing the practicality and economics of an on-line inquiry system to the subscriber/administration base....

This is the London project. It is in the process of evaluation, with a report that basically says it is practical, that it is of benefit to the staff and the economics look reasonable. The next stage, as far as we are concerned, will be one, technical. Which is to address the communication and technology problems of such a system across the province.

Secondly, the operational procedural security type of issues that we will want to look at in terms of level of security and protection of data.

Those are the next two immediate steps. I believe the OHIP management team have accepted a draft report describing the practical and economical approval.

The OHIP on-line inquiry system was eventually approved and is now in operation in OHIP district offices.

None of these difficulties is insoluble from the viewpoint of computer security. But the correction of all potential methods of breaching a computer systems security wall is an expensive proposition. It is true that no perfect system can be accomplished. Mr. Milne of IBM Canada, Ltd. made this point at our hearings:

You cannot prove that something that cannot be a hundred percent secure. It is only a relative level of, I have invested enough to make it this safe, which means that the level of investment that somebody has to break my schemes is relatively high....I would hope personally that our society is not getting to the point where we have to be investing at an uneconomic level on the assumption that no one can be trusted. I think ultimately any system is going to depend not on the technology, it's going to depend on the people.

That company's brief put it this way:

While total security may not be attainable, a level of protection appropriate to user needs can be achieved in automated systems by proper attention to the subject.

It is well known that the degree of removal of exposure follows the law of diminishing returns relative to the amount one is willing to spend. Each successive increment of security becomes more expensive than the last increment. In economic terms, this means that one must carefully determine the perceived threat to the system in order to select a level of security which is affordable.

What are the reasons for concern about the security of health information on computers? It must be remembered that there are different spheres of interest in health data. First, there is the source of data, the patient. The patient thinks of the information as being confidential between him or her and his

or her physician or physicians. Next, there is the physician or the data receiver. The data receiver acquires information in order to make diagnoses and develop therapeutic plans. The data receiver may also perform research using patient information, especially in teaching institutions. Finally, there is the data guardian. The data guardian is the person or group of persons entrusted with protecting data wherever it may be stored. For example, in paper medical record systems the data guardians are the health-care providers and the members of the medical records department. In the health insurance schemes, the data guardian is the insuring agency. In a hospital with an automated patient record system, the data guardian might well be the director of the computing centre.

The reasons for concern on the part of the sources, the receivers and the guardians of medical data or information are explored in what now follows. One factor is the sensitivity of data sets. One must recognize that unwarranted access to certain information about an individual, or the mere knowledge that an individual is a member of a specific class, would be perceived by that individual as a violation of his or her privacy. If a patient is required to give information and then becomes a member of a data set, for example of persons with venereal disease, or of persons who have undergone psychiatric care, the mere fact of that information becoming known to others can embarrass the patient, unreasonably prevent him or her from undertaking certain types of professions (such as politics), or can compromise his or her image, even though the reactions to that information may be irrational on the part of the public. Another factor is the data guardian's responsibility as perceived by individuals concerning the privacy of any information entrusted to another. Again, medical information is believed by individuals to be privileged material shared only with the physician or as locally as possible within the health-care environment. Anyone who comes into possession of this information, even by virtue of being the director of a computer centre, must answer for the role that is perceived for him or her by the sources of data.

Whenever we are made aware of an actual breach of our security systems, whether the breach be for fun or with anti-social intent, both the public outcry and the compromising of our presumed control over access to our systems raise our awareness concerning exposure. They also indicate in concrete terms that precautions have their place in the light of the documented real threat. From a patient's point of view we have been lucky in this regard in the past in that no real violations have been detected. From the data guardian's point of view this may be considered less than lucky since the absence of documented

breaching of the security system creates the feeling that the issue is exaggerated, that the cost is not worth it, or that the precautions taken are adequate. To a certain extent, we have been lulled into a false sense of security.

Perceived threats are also important. The public's imagination about the ease with which our systems can be penetrated, or our own recognition of how much havoc a determined intruder could wreak, force us to face unanswerable questions about the responsibilities of the guardians of data. Since some of the information stored is sensitive and much of it is shared in confidence, perceived threats lead to a state of anxiety and perhaps, in some cases, to at least a minimum standard of computer security.

It is important that we look at each of these factors in greater detail and relate them to real circumstances. The first is the sensitivity of data sets. A data set is simply a collection of data. By sensitive we mean that an individual would consider it a violation of his or her privacy if the data were accessible to anyone other than the health-care provider. In the course of examination and treatment for medical problems each of us is not infrequently placed in the position of having to share information with a health-care worker which we would consider sensitive or at least potentially embarrassing. Sometimes the information can, in fact, jeopardize our professional status, affect our ability to obtain insurance, or affect us in our relationships with other persons. Most people would perceive psychiatric or psychological information to be particularly sensitive and many would consider information relating to sexual activities to be potentially embarrassing as well.

Less frequently, perhaps, we may be put in the position of identifying ourselves as a member of a given class of patients, in respect of which the mere fact of being a member of the class would be embarrassing. At times we may supply information which in itself is not embarrassing, but which could compromise us if it were used as a means of obtaining other data about us. For example, in providing sufficient information for OHIP billing, our personal identification data can be used as a means of linking OHIP records with other health information about us not related to the treatment we received. Linkage data can even allow completely unrelated files to be located and searched. This is possible, for example, if we supply our social insurance number for the purpose of registration on a hospital admitting system, and then this social insurance number is used to obtain other information, for example, from motor vehicle registration or from tax records. This latter problem is even more insidious if, by chance, we are mislinked to information and become known



to one or other agency as being a criminal or a child beater, when in fact this erroneously identified information was mistakenly correlated with accurate information. It should be clear from these observations that many kinds of data can be viewed by individuals as being sensitive either directly or indirectly. The patient's privacy can be threatened when almost any data-collection system is undertaken, most especially when individuals are personally identified.

With respect to the data guardian's responsibility as perceived by individuals concerning the privacy of any information entrusted to another, regardless of what we may feel is sensitive data from the viewpoint of the patient, or of what the guardians of data or the providers of care consider as sensitive data, it is generally expected by the public that any information shared for the purpose of treatment is to be kept strictly private, with only the most local circulation necessary for good quality of care. If the information is eventually publicized or utilized for linking together other data sets, either through mistake or misdeed, it will be perceived by the individual as a violation of his or her privacy. It will not matter whether the violation was achieved through direct access, through erroneous linkage, through the loss of computer media, or through paper transfers of the data to another person not involved in patient care. In collecting health data and in storing it, institutions and individuals become involved in this implicit (and at times unworkable) agreement concerning the patient's privacy.

Many opportunities exist for the violation of this understanding. For example, data collected may be utilized for research purposes and inadvertently published. Any researcher may retrieve selected information from a data base and obtain subsets of patient data that are or may easily be identified with individual patients. Information collected for one purpose, such as follow-up, may find itself in another's hand whose intentions are good (they may be interested in rehabilitating post-surgical patients), but whose participation in the patient's care was outside the implicit initial contract with the patient. Especially given the large numbers of people who in some systems handle data, the potential for offending the perceived confidentiality of information is great.

Turning to real violations of privacy, there is nothing like an occurrence of this sort to create a situation of public clamour and organizational panic concerning the breach of the security system. As suggested before, we have either been blessed by the lack of clear-cut occurrences or lulled by the lack of knowledge of existing violations.



One issue which received particularly intense public interest was the alleged illicit access to the venereal disease data base known as the "VD fun run". A former employee of a computer service company, a computer technician, claimed that he was present when access was obtained to tapes of the venereal disease file and the tapes were linked to OHIP claims files in order to turn up information about patients who were on the venereal disease file. The claim was the subject of a story written by Globe and Mail reporter Richard Furness that appeared in that newspaper on November 1, 1977:

A technician who worked at the Government's Leaside Data Centre last winter said in an interview that programmers often run fun tests through the computers in slack moments. One such test, he said, produced names of and personal information about people suffering from syphilis.

. . . . .

The technician said that in last winter's "fun test", the VD tape and the Ontario Health Insurance Plan data base were used on one program to see whether it would combine information from both, providing names of people suffering from syphilis, their addresses, age, sex, marital status, OHIP account numbers, and whether the disease was in its primary or secondary stage in each person.

. . . . .

"As you can see, the permutations are many and the potential in the wrong hands is considerable," he said. "Yet all this information has been run and there are no checks to see if the information is abused."

The computer technician making the claim was Jon Hewson who testified at our hearings where it became clear that he had fabricated the story. The following exchange between Mr. Strosberg and Mr. Hewson is taken from a transcript of the hearings:

Q. I am suggesting to you that you have never seen a list of the names of persons

who have had venereal disease, with their address, their OHIP code, have you?

A. I have seen long lists of what they had, but it's not my concern.

. . . . .

Q. Did you ever think that any such list was made by anyone running a tape in the time frame that you have described to us?

A. No.

Q. If you told Mister Furness that, it would be a lie?

A. Yes, it would.

. . . . .

Q. What we have read here is what you believed was theoretically capable of taking place. Not what you knew actually had taken place.

A. We discussed the dangers of the setup as it existed and what could be done.

Q. Yes. The theoretical abuses?

A. Right.

Q. Not what you knew in fact had taken place?

A. You are discussing what the dangers were.

Q. Yes. But not what had taken place?

A. Not at the time I worked there.

MR. COMMISSIONER: Do you mean by that that it had taken place at some other time?

A. It could have done.

MR. COMMISSIONER: No, no. But we are not talking about what could have happened. You said that you were not discussing something that had taken place during the time you worked there. I understood you to mean it had happened at some other time.

A. It's just that so many other things happened that shouldn't have happened. It could easily have happened at some other time.

MR. COMMISSIONER: Did it ever, did you ever hear that it had happened at a time other than the time you worked there?

A. No.

Nonetheless, access to the venereal disease files themselves was quite possible, as the tape library was accessible to virtually anyone and the tapes themselves were not protected by any password system prior to this revelation. Allan Ross, a systems specialist in the Management Systems Branch (then known as Systems Management and Co-ordination (SMAC)) of the Ministry of Health, gave this evidence at the hearings:

Q. So that if you were to link a VD tape with an OHIP tape, it would be necessary first to do, is to convert all the VD numbers to OHIP numbers or vice versa?

. . . . .

A. You would have to establish some kind of, method of linking the two files. I think that's what you are asking me?

Q. Yes. Is that not correct?

A. That is correct.

Q. As I understand it, and from what I have heard from anyone that I have talked to about it, that's just given time and given unlimited time and unlimited money, it might be possible to do it. But in the absence of that, it's practically impossible?

A. Yes.

. . . . .

Q. Now dealing with the theoretical portion of the evidence, you said earlier that there was no password in November of 1977?

A. Prior to the article.

. . . . .

Q. In November of 1977, is it fair to say that this tape management printout would be accessible to anyone who worked at the Data Centre?

A. Yes.

. . . . .

Q. Because there is no password and because he himself had access to the computer, he then can be in a position where for example the venereal disease tape could be put up on the computer?

A. Yes. Prior to that article.

. . . . .

MR. COMMISSIONER: Is it fair to say that we can thank Mister Furness for the security that came out by the introduction of the necessity for the password?

A. Yes.

The publicity surrounding this event had the salutary effect of tightening up the system.

During the course of our inquiry it became clear that the entry of a patient's name into the venereal disease file is anything but highly selective, since some of the tests used to detect venereal disease can falsely indicate a positive result, thus possible bringing about entry to the registry, despite the fact that the patient may not have venereal disease. It was also revealed that personal identification information was kept on the files and a great deal of additional data not really serving anyone were captured since it was convenient to do so. In the light of the sensitivity of the information, it is not

unreasonable to ask whether such a data base should be allowed to exist at all and, if it is allowed to exist, whether the patient identification should not at least be kept separate so that only absolutely essential medical information is stored. Further consideration of this subject is found in the discussion of compulsory reporting.

In connection with the issue of perceived threats, almost anyone with a basic knowledge of computer systems can fantasize how access to a computer system might be achieved. However, in order that a perceived threat be considered as a stimulant for improving computer security, it must have the following characteristics:

1. It must be believable, that is, there must be someone who needs, values, or wants the information.
2. It must be achievable, that is, someone must be willing to try to get the information or to get others to obtain it. There must be some flaw in the security system which will permit a determined intruder to obtain the desired information.
3. It would be best if the violation were undetectable, that is, that the violator could get away with the illicit access, or at least that the violation be detected slowly enough that the violator can escape. If, however, the violation is truly undetectable, a situation which would be true in the case of many non-secure systems, no one would ever become aware of it.
4. It must be repeatable, that is, the violation would best not be a unique occurrence, but would be able to be undertaken at will.

Clearly, we are dependent on those who are thoroughly familiar with computer systems for the evaluation of potential threats. If they choose not to reveal to us the system's potential weaknesses, then such weaknesses will never be corrected. This gives rise to a conflict since, by making weaknesses known, the potential increases for someone to utilize a back door. Some have argued that the best solution would be to train individuals in the area of "breaking computer systems". While keeping them on the side of good, we would be able to discover the real weaknesses in our computer systems. At the present time such services are offered by agencies, but such agencies are expensive and few and far between.



It is apparent that perceived threats are real threats that luckily have not yet happened. Some perceived threats came to our attention during our inquiry:

1. The venereal disease file access was in fact shown to be a perceived and not a real threat. Only part of the story could, in fact, have been carried out, but the threat pertaining to that part alone was sufficient to cause corrective action. It would, indeed, have been possible to obtain access to the venereal disease tapes and either to copy or peruse the information.
2. The OHIP system has been shown to be weak in security at a number of key locations as documented in the study carried out for us by Peat, Marwick and Partners and which is discussed at greater length in the section of the report describing the Ontario Health Insurance Plan. Almost any computer system that might be studied could be shown to be in the same position, at least to some degree.
3. Although the security on the government services system was shown to be, relatively speaking, excellent, the fact that the hospital records of one hospital, York Central Hospital, are on a computer which serves other purposes should lead one to question whether a determined intruder could link hospital records with other data.
4. The Hospital Medical Records Institute (HMRI) system processes and stores hospital in-patient data for about 250 Ontario hospitals and produces statistical reports and indexes with information provided in identifiable form. This system and some of the concerns expressed by the Ontario Hospital Association and others are dealt with in the section on the Hospital Medical Records Institute.

One can raise the spectre of perceived threats with almost any computer system. The task must be to eliminate as many as possible of the perceived threats which are likely to be embarrassing to patients and in respect of which the cost of successfully doing so is acceptable. It is thus necessary to assess the level of threat before the danger can be quantified and the cost of preventing it justified.

The present situation is one in which all factors favour the gatherers and guardians of data, and in which the privacy of the sources of data is not sufficiently protected. During the course of our hearings the following facts emerged:

1. There are no controls regulating who may establish a medical data base and create a collection scheme.
2. Neither the data receiver nor the data guardian is put in a position in which either must defend why the data is being collected and what the quantitative need is for each data item.
3. The receiver of data may not be aware of the uses to which the data will be put, who the user will be, where the data will be stored, or the reasons for collecting, storing and processing the data.
4. The data guardian does not have a set of rules or guidelines defining his, her or its responsibilities for protecting the data with which he, she or it is entrusted.
5. The real degree of threat to stored data is not known and it is therefore difficult for the data guardian to establish and to justify the cost of a sufficient level of security.
6. The source of data, the patient, often does not know why data is being collected from him or her, where they are being stored, into whose guardianship they are being transferred, what protection of his or her privacy is accepted, and which other groups or agencies might have access to his or her data. He or she, in fact, may not be aware that his or her care is not linked to the giving of any or all information requested at any point in the health-care process.
7. The patient does not know to whom to direct questions or where he or she might redress grievances if he or she is injured in any way through the release of information concerning him or her.

Neither the patients nor the agencies collecting and keeping data know which way to turn and what their privileges and responsibilities are.

Patients are at the mercy of the data-collection organizations who have the resources, the money, and the ability to deny services. The data-collection organizations determine who must give information, what information must be given, where it is stored, at what level of security, and so forth. The speed of development of systems has widened the gap between what the patients perceive as the meaning of confidentiality and what in fact happens using large systems. There must be created a

minimum standard which should be required of any person or organization who is in the position of being a guardian of medical data.

*Recommendations:*

36. That, before the establishment of any medical data base, the person or agency who will be responsible for protecting the confidentiality of the information carry out the following requirements:

- (a) State the purpose for which the data are being collected, indicate the class or classes of patients in respect of whom it is being collected, and list all data items to be included.
- (b) Set out the quality control procedures which will ensure that data are accurately collected and properly linked to the correct patient.
- (c) Set out all physical and software security procedures (suggested details of which are listed in the following section) to protect the data from unauthorized access or destruction. Security should be required to meet a standard corresponding to the sensitivity of the information stored.
- (d) Designate the person directly responsible for protecting the confidentiality of the information, to whom violations of any individual's privacy are to be reported.
- (e) Show that all persons who have access to data have been informed of their responsibilities for confidentiality and that a system exists for protecting the confidentiality of the data.

(f) Specify to whom and where such data may be transmitted, circulated or otherwise given.

(g) Define the special and ultra-secure procedures associated with personal identification data and the methods by which it is guaranteed to be kept separate from other data.

37. That the names of medical data bases and the files they include, an itemization of the contents of the files, and the names of those responsible for their maintenance and safekeeping be centrally registered in a data base, public access to which is available.

38. That a set of minimum guidelines be established for the security of specific kinds of medical data base systems. (There may be several classes of systems, such as data bases collected and kept within an institution, multi-institutional data bases, and province-wide or nation-wide data bases.) Data bases may also be classified according to the sensitivity of their data, the size of the data base and the potential for linkage of multiple data sets of different types. The minimum guidelines should specify the minimum physical security for access to the system and its terminals, the kinds of minimum software security implemented in the data base software, and the methods of backup and duplicate logging in order to protect the data base from deliberate or inadvertent destruction.

39. That any data about a given patient kept on a medical data base used in patient care be available for review by the patient on request. There should be a mechanism for correcting data or at least indicating that the patient and the receiver of data differ about a given item.

40. That procedures for the purging of data, the destruction of media and the keeping of copies be established both for long-term systems and for systems which exist transiently in support of limited-term projects.

41. That an ombudsman of medical data bases or the equivalent be appointed to act as an overseer ensuring that the rights of the individuals are protected, that grievances can be redressed, that violations can be detected and that the guidelines are kept up-to-date.

42. That there be:

(a) a regular review of all systems and a constant updating of the list of responsible personnel and the contents of data files;

(b) a means of ensuring that problems are corrected and that violations of patient privacy are addressed;

(c) a mechanism for the updating of procedures with new technologies; and

(d) a means of publishing documented violations, important potential violations, or suspected violations of computer system security whenever they are detected.

Knowing how easy it is to remove and destroy paper records and how undetectable that kind of mischief can be justifies the conclusion that computers are a whipping boy. Yet, they do create new and more sharply defined problems and thus may cry out for regulation. Similar action could equally well have been directed at our paper record systems. Computers themselves are not the problem; they have simply made the problem more clear, more immediate, affecting more of us, and putting more at stake. In the final analysis, the real issue is what we store on computer systems and how we or others use it. Computer systems make it easy for us to get large amounts of information and to use it in ways which were never intended by the person who provided it.



By and large, in dealing with the potential exposure afforded by computer systems, prevention is the best protection. We should recognize the dangers, work out the weaknesses or discover them by testing our systems, keep the number of people who handle data to a minimum, and as much as possible act on a "need to know" basis. Once information systems have been properly registered, one should really say little more about them and certainly not broadcast details about them. Finally one must recognize that accountability to the public is now expected of the information receiver and the data guardian. It must be demonstrated that at least the minimum standards for data security are being met.

The security measures which should be employed in protecting data from unwarranted access or destruction should be balanced against the potential threat and the sensitivity of the data stored. The following measures have been proposed by Mr. Covvey as minimum requirements without which a data base of almost any kind cannot be considered secure. As a non-expert, I am persuaded that they are eminently reasonable and put them forward for consideration. Any items indicated by an asterisk (\*) can perhaps be deleted for all but the largest and most sensitive data bases.

### Physical Security

Physical security measures relate to the prevention of access to or destruction of the computer system itself, its terminals or its input, output or storage media.

The following are the key physical security methods.

1. All areas which contain computer systems, terminals, or stored media should be locked, and keys should be provided only to those who have a need to access these areas. Many computer installations will utilize one of a variety of electronic or cardactuated locks. These provide the ability to easily change the codes as personnel leave or when the codes become compromised.

Staff must be properly trained to make sure that this basic security system works, since if they leave cards lying

about or prop open doors, the entire system is ruined.

2. Terminals should be provided with locks which will ensure that only authorized personnel can turn the terminal on and use it.
3. Areas where media are stored should be locked and tape and disk libraries can be provided with a librarian and/or a computer terminal which forces the checking in/out of the media before they will be accepted by the computer.
4. The computer area as a whole should be kept off main floors and not put in full view of casual observers. If at all possible, the access area should always be occupied by at least one person who may serve as a receptionist for the computer area, or, for small systems, for some other area.
5. All personnel and visitors should be provided with identification badges, some of which can be utilized as a method of unlocking doors if desired.
6. All personnel entering a computer room or a media storage area should be accompanied no matter what their reason for access. Making it necessary for at least one other person to be present significantly reduces the probability that the system can be compromised in that it ensures that at least one col-laborator is necessary.
- \*7. Programmers should not, in general, be permitted in the computer room. Only operators should be permitted access whenever such a rule is possible. Secretaries, service personnel, etc. should always be accompanied by appropriate personnel during whatever period of time they are allowed access to the computer room.

8. A logging in and out procedure should be employed for every access to the computer areas for whatever reason. The simple keeping of a registration book at least allows access to be checked. The computer media themselves should never be allowed to leave their protected areas or the data library, except as required in the computer room itself.

These media should never be permitted outside the immediate building for whatever reason. The exception to this is the storage of duplicate or backup files in another secure area to protect them in the event of fire.

#### Fire Prevention and Protection from Data Destruction

Although properly under the title of physical security, the area of fire prevention is separated for convenience. The object of these measures is to prevent complete destruction of the computer equipment or at least of the data in the event of a fire, flood, terrorist action, or other natural or man-made disaster.

#### Software Security

A variety of methods can be introduced into the computer system programs to reduce the likelihood that unwarranted access or destruction can occur;

1. Wherever possible, terminals should be restricted to accessing specific data sets and to performing the minimum set of operations which is in keeping with the functionality required at that terminal.

For instance, a terminal in an enquiry area should only be able to examine data not alter it, and then only examine those records which are relevant. Terminals can be designated as read-only, data input preparation only, etc.

2. A user should be required to sign onto a terminal utilizing a proper account number or departmental identification code. In addition, each and every individual user should be required to utilize a password whose exact characteristics are known only to that user and which may be changed at will when it appears that the system has been compromised.

The usage of names and other easily discoverable passwords should be prevented by requiring a mixed alphanumeric scheme.

3. Once a computer has the ability to access data there should be record-level access protection so that if it is desired to prevent access to personal identification data or other information, this can be prevented.
4. All accesses to the system should be registered on a transaction log including the time of access and the access codes used. The transaction log should also keep a record of all transactions executed. There should be time restrictions on the utilization of given user codes or terminals to prevent unwarranted access. Multiple attempts at different codes at the same terminal within a short period of time should result in an alarm to the system's supervisor. In addition, that terminal should be locked out from further service.
- \*5. Serious consideration should be given to encrypting all sensitive data bases or at least the highly sensitive portions such as identification data. If a sophisticated encryption mechanism such as the NBS encryption algorithm cannot be used, at least basic scrambling of the data should be accomplished to discourage intrusion.

6. All transactions to remote terminals should have a mechanism for checking the identity of the terminal through hardware installed in the terminal. The terminal's identification can then be accessed by the system before any data is transferred to or from that terminal.
7. Remote terminals should be especially restricted in terms of the operations they can perform.
8. Basic software security techniques should be practised in the operating system and in the applications system software. When records are returned to a user area in the computer, these should be devoid of pointer information which permits access to other data.
9. Identification data should be kept in separate files and only available when absolutely essential such as for the input of information in order to check that the appropriate linkage of the new information is being effected. The identification file should be the first one encrypted if this method is utilized. Access to this file should be strictly controlled and no output of personal identification data on paper or magnetic media except under the most controlled circumstances should be possible. Wherever possible, information on the system should be collected without personal identification data.
10. When reports are produced of a statistical variety, proper rounding off of the numbers should be utilized to ensure that records cannot be identified with an individual, or at least that it is extremely difficult to do so.

#### Personnel Security

The people who use a computer system must also be controlled. The following methods are suggested:



1. Every person participating in the guardianship of data should be required to take an oath of secrecy and be provided with a statement indicating that person's precise ethical position.
2. When a computer system is used to process data given in confidence, those responsible for the processing of data must preserve this confidentiality, that is, the duty of confidentiality transfers. This is intended to counteract the usual situation in which the farther the data is away from the provider, the lower the feeling of responsibility for that data.
3. Persons in especially sensitive positions should be screened and the sensitivity of their position should be emphasized.
4. Only personnel with a need to be in a given area should be permitted access to that area, the same being true of all media, terminals, and data.
5. When persons leave a facility, locks and passwords should be altered.
- \*6. In highly sensitive data bases, professional security personnel should be utilized to guard the facility and professional security testing agencies should be employed to ensure that the system is secure at a sufficient level.
7. Personnel should be encouraged to identify and rectify all potential security weaknesses of the system.
- \*8. Whenever particularly sensitive data or access to computer facilities is necessary, jobs should be carried out by pairs of personnel.

No security system can be perfect. However, many rather simple measures can make the system a safer one. Only if the responsibility of the data guardian is recognized, however, will

the cost of instituting security measures seem justified. Care and common sense can do much to improve almost any system. Smaller computer systems within hospital departments or even offices must be specially recognized as targets for these considerations. It does not matter whether one is dealing with a microcomputer, a minicomputer or a large computer. Perhaps the most important consideration of all is the simple raising of awareness of all the staff about the potential for intrusion. It is not enough but it goes a long way toward making systems more secure.

## APPENDIX: DEFINITIONS

The following definitions are provided for persons unfamiliar with some of the language used in connection with computer systems and their security.

More exact and general definitions can be found in a variety of data processing dictionaries.

Access. The process of gaining entry to a facility or of gaining possession of a data item. "Accessing" data on a computer usually means obtaining it for reading, or copying so that it can be carried away.

Accountability. Accountability is the responsibility to explain and to correct for failures in any process. With satisfactory privacy legislation, an agency would be accountable to the individual by ensuring the individual that his or her data had been kept in confidence.

Data or data item. An individual piece of information which describes some aspect of a patient, his or her disease, or his or her treatment. For example, the diagnoses associated with the patient are data items. The patient's name is a data item. Data on a patient are the sum total of all the data items.

Data entry. The process of putting data into a computer system.

Data guardian. The data guardian is that person made responsible for keeping data. In a paper medical record system, the members of the medical records department are data guardians. In a computer system, such a responsibility may fall on the director of the computer centre, or another responsible official in the organization. It is recognized that often the data guardian is different from the data receiver, who, in the medical instance, is usually the physician.

The data receiver. The data receiver is a person, such as a physician, nurse or social worker, who receives the data from the data source. This person either utilizes the data immediately or participates with others to bring the data to bear on the health problem of the providing individual.

Data retrieval. The process of obtaining data stored in a computer system or of obtaining access to it.

Data quality control. Data quality control refers to the process by which one ensures that the data collected are correct and as complete as possible. This may be accomplished by ensuring that items are of the proper length (such as social insurance number being nine digits), that names are alphabetical, and that inconsistencies among data items are not permitted, as, for example, a pregnant male.

The data source. In medicine the data source is usually the patient, although sometimes it may be the patient's relatives or guardians. This is the person who makes data available, usually for the purpose of assisting in a medical investigation or in support of medical treatment.

Data base system. A data base system refers to a software system (programs) designed to provide a means of storing and retrieving data. Data are stored in files which are collections of records of similar types (for example, the admitting file is composed of admission records) and each record is made up of data elements or data items such as patient name, address, telephone number, and so forth. A medical data base is used to store medical information. Data bases are established to reduce the redundancy of stored information by making a single item available to a variety of different users. As such, data base systems are designed for sharing. A data base system should provide a standard method of storing and retrieving data, basic security capabilities such as password access control, and standard programs such as retrieval language often called a query processor. The files in a data base are organized in a way that suits the use to which they are put. A data base is a systematically arranged collection of files and its organization often reflects the way in which an organization makes use of its data.

Data set. A data set refers to a given collection of records about a patient. For example, a surgical data set is a collection of records relating to surgical events and an oncology data set is a collection of records relating to cancer diagnosis.

Encryption. Encryption refers to the process of taking a message and changing it into an apparently meaningless sequence of characters, in such a way that the message cannot be read except by the intended receiver who knows how the message was changed. The word 'encrypt' is synonymous with the word 'encipher'.

Exposure. The word exposure refers to those aspects of an organization which are susceptible to compromise or breaching by an intruder. An agency has an exposure in a given process if that process is able to be compromised, the data illicitly obtained, or undesired persons informed when that is not in the interest of the agency.

File. A collection of related records.

Hardware. The computer system itself, the electronic and electromechanical parts.

Linkage or record linkage. Linkage or record linkage refers to the process by which two independent records can be found to correspond to the same person and thus be brought together as a related data set though, prior to the linkage, they could have been unrelated. This can be accomplished through the use of a standard identifier associated with each of the records where the matching of this identifier allows their linkage, or it can be accomplished through a number of data items being similar for each of the two records such as the same last name, the same birth date, the same sex, etc.

Program. A series of instructions which cause a computer to perform some assigned task.

Record. A collection of related data elements or data items. An admission file may contain admitting records, each record being composed of the patient's name, address, telephone number and so forth.

A registry. A registry is, for present purposes, simply another name for a medical data base, usually one which is put to work for some particular medical service or research purpose. For example, a tumor registry may be utilized to obtain epidemiological statistics on all persons who have cancer. A surgical follow-up registry may be utilized to provide a means of easily following up patients over many years to ensure that their disease is controlled.

Security. The security of a computer system refers to the ability of the computer system to withstand the penetration of an intruder. Computer security also refers to the protection of

the data on a computer system and the media on which data are stored. Most often one speaks of physical security and logical security. Physical security relates to preventing physical access to data, computers or media. Logical security refers to software methods which prevent the use of programs or the use of data unless the identify of the user both permits access and allows the required type of utilization.

Software. The programs that process data on a computer system.

Trojan horse program. A program which has been hidden in a larger program. It normally remains completely inactive, but it can be activated at will by an intruder. Once activated the Trojan horse program can access, delete or modify data, set up false accounts or debit existing accounts, or even destroy a data base.

Unique identifier. A number or alphanumeric code which refers exclusively to a given individual, is known by that individual, and is utilized to ensure that records about that individual are all linked to his or her proper identification record in a computer system.



# The Hospital Medical Records Institute

When we first began our investigation of computerized health information, we gave special attention to the Ontario Health Insurance Plan system as being the single most extensive collection of health information in the Province. There is, however, another very large data bank maintained by the Hospital Medical Records Institute, usually referred to as HMRI, which is a private non-profit data processing organization based in Metropolitan Toronto. HMRI processes data on hospital in-patients and produces statistical reports and indexes for hospitals. The Institute also produces a tape of all the Ontario data for the Ministry of Health. The Ministry file is called the Ontario Data File, but it is often referred to as the HMRI file.

A brief historical account will help to clarify HMRI's role in relation to hospitals and the Ministry of Health. The Institute was established in 1963 as a partnership between the Ontario Hospital Association and the Ontario Medical Association. The Ontario Association of Medical Record Librarians (now called the Ontario Health Record Association) was accorded observer status. From its inception in 1963 until 1973, it functioned simply as an optional service for individual hospitals, providing them with statistical analyses as an aid in administration and monitoring of health care within their institutions. In 1974, the Ministry of Health made it mandatory for acute care hospitals in Ontario to subscribe to HMRI and for HMRI to relay to the Ministry all the data collected, so that comprehensive information in a uniform format would be available for government use in planning and research.

Between 1963 and 1973, HMRI processed data for about 50 institutions, most of them in Ontario. In 1974, HMRI's clientele expanded dramatically to about 250 institutions, as a result of the Ministry of Health requirement that all acute care hospitals subscribe to the service. The Ministry arranged to finance the hospitals' participation in the programme through their budgets; the hospitals pay HMRI out of this allotment at a fixed rate per patient discharge. The sudden increased enrolment in 1974 had a profound effect on HMRI; a financial crisis ensued and report production faltered badly in both

timeliness and accuracy. Outside consultants were hired to help put the Institute back on its feet. It took until January, 1978, for production to return to normal. The Ministry of Health helped HMRI through the recovery period with funding and consultation. In 1975, the main computer processing passed from a private subcontractor to the Ministry of Government Services, which continues in this capacity to the present time. The support of the Ministry of Health was crucial to the survival of HMRI, since the hospitals were growing understandably dissatisfied with the service they were receiving.

In 1977, HMRI became a federally chartered corporation. The charter stipulates that the Board of Directors consist of 14 members, the OMA and OHA each appointing seven of them. The OMA nominates three physicians, the OHA three hospital administrators; each association nominates one person from the Ministry of Health, one person from the Ontario Health Record Association, and two outside directors who are not associated with the health field.

Since 1978, HMRI has been able to achieve an internal turnaround time of less than a week for reports to hospitals, and its computer programs have not been unduly plagued with errors. The new program of reports introduced in 1978 remains in effect to this day. In 1979, the Ministry added chronic care hospitals to the group of hospitals required to report through HMRI. Currently HMRI produces reports for over 300 institutions, of which only a handful are outside Ontario.

The HMRI file contains very detailed clinical information about all in-patients of Ontario's public and private hospitals of the following types: acute care hospitals, including chronic care and rehabilitation units; chronic care hospitals, including rehabilitation units; and all rehabilitation hospitals, including chronic care units. Private psychiatric hospitals are also included. The foregoing types of hospitals are required by the Ministry to report information through HMRI. But if any other Ontario institution uses HMRI services for its own data processing, its data are also incorporated into the Ministry's HMRI file. In this category at the present time are Royal Ottawa Hospital (psychiatric unit), the Alcoholism and Addiction Research Foundation (in-patient unit), and out-patient units of about 20 active treatment hospitals.

Whereas OHIP health data encompass a wider range of patients (the HMRI file, with a few exceptions, pertains only to hospital in-patients), HMRI data are far more comprehensive. How comprehensive will be evident from a description of the computer input document, which is called the HMRI abstract. The

HMRI abstract is filled out by a hospital's medical record department upon the discharge (the term includes death) of a patient. Patient identifiers on the abstract include the patient's OHIP number, hospital register number and chart number, and date of birth. The patient's name does not appear on the abstract. The one-page form covers a wide range of specific health information: details of admission and discharge, physicians (as many as six) and the services they provided, diagnoses (as many as sixteen); procedures by date (as many as twelve) along with the physicians who performed them, additional services, such as type of therapy, services of a social worker, or provision for home visits by a nurse upon discharge, and weight (mandatory only for newborns and infants). The foregoing data must be provided by requirement of the Ministry of Health. Further data are optional, to be recorded according to the needs of the individual hospital, and include service transfer information, if the main responsibility for a patient's care changed hands during his or her hospital stay, whether a special care unit, such as a coronary unit, was involved, reference to pre-admission testing or examination, infection history, specifying when an infection occurred, information about blood transfusion, and any extra details on procedures performed relating to tissue, time, operating room, anaesthetist or technique. At the end of the abstract is an optional section for hospitals to process whatever data they wish. All the data, whether mandatory or optional, are captured for the Ministry's HMRI file.

After processing, the data are kept in two forms: by hospitals, in the form of statistical reports and indexes; by HMRI, on a computer tape; by the Ministry of Health, on a computer tape. The computer tapes incorporate all the data on the abstracts. HMRI's own file differs from the Ministry's HMRI file in one main respect; it includes data from the few out-of-province hospitals that are also clients of HMRI. Hospitals receive from HMRI a variety of monthly, quarterly and annual reports derived from the data on the abstracts. Each month they receive a listing that displays all the coded data for each discharged patient in order of hospital chart number, a statistical analysis of discharges grouped by patient services, and indexes of patients grouped by diagnosis, procedure, and type of service. Quarterly, they receive an index of patients grouped by physician, and statistical summaries analysing length of stay by various groupings: diagnosis, procedure, patient service, physician service, and physician. Annual reports are cumulative versions of the discharge analyses, indexes, and length of stay reports described above. In addition to these standard reports, hospitals may arrange for special reports under the Special Needs and Applications Program (SNAP) of HMRI. The most common need for special statistical analyses arises in preparation

for an accreditation review. Hospitals may also request print-outs of any data in the HMRI file which originated in their hospital.

Almost all information on the abstract, and in the processed forms, is coded, with the exception of birthdate and dates of admission and discharge. The contract between HMRI and the Minister of Health specifies the code to be used for diagnoses and procedures:

Reporting of diagnoses, external cause of accident and procedures will be in accordance with ICDA-8 and, as of April 1st, 1979, in accordance with the World Health Organization International Classification of Diseases, ninth revision (ICD9), and the Canadian Diagnostic, Therapeutic and Surgical Procedures Classification.

Other mandatory data are coded according to the HMRI manual. Optional data may be coded as suggested in the HMRI manual or hospitals may devise their own codes. The hospital is identified by the number assigned to it in OHIP's Physician and Hospital Index. Physicians are identifiable by a number assigned at the hospital concerned. (The Ministry of Health has considered asking for a change to the physician's OHIP number, but no action has been taken.) Patient identifiers include the register number, chart number and OHIP number. A register number is assigned to every patient in sequence of admission pursuant to the provisions of sections 18(1) and 19 of Regulation 729, made under the authority of The Public Hospitals Act, R.S.O. 1970, chapter 378. The chart number is a number assigned to a particular set of patient records by a hospital. In most cases chart numbers form a discrete number system, but in some hospitals they are derived from register numbers and in a few hospitals the Social Insurance Number is used. Indexes of register numbers and chart numbers are kept at every hospital. The OHIP number is listed with the patient's name in the OHIP enrolment file, which is accessible on-line to OHIP district offices.

HMRI data are individually identifiable in all forms, except on those of the hospital reports that are statistical. The identifiers in use provide several ways of uniquely identifying an individual. The patient's OHIP number by itself is not unique, since it could represent all the members of a family. However, the OHIP number does provide unique identification when used with some other personal detail such as birthdate. The hospital number together with the register number begins again



at the number "1" each year. Therefore, if the year of origin of the data is not known, the date of admission or discharge is also needed for unique identification. Hospital number and chart number together are another possible means of unique identification. In those few cases where the Social Insurance Number is used as the chart number, this number alone constitutes a unique identifier.

Since October, 1978, the Ministry of Health has maintained an additional file, in which all the Ontario HMRI data are linked with the OHIP 106 file. The 106 file contains only basic information, almost entirely non-medical, about admission and discharge of hospital patients. The linked records are known as the H/6 file. The purpose of the linkage is to incorporate the patient's name with the HMRI data. If the name is a common one, then some further data item is needed to provide unique identification. All the other identifiers mentioned above are also stored in the H/6 file.

Our investigation with respect to HMRI satisfies me that the Institute has conscientiously carried out its objectives with due regard to the confidentiality of data that are processed. However, there are issues that must be addressed, some requiring immediate remedy, others strongly suggesting a need for policy review. Concerns relating to HMRI were expressed to me by hospital administrators, health record administrators, and physicians, particularly through their professional associations. These associations submitted thoughtful briefs and appeared at our hearings. They are aware of their responsibilities under legislation and under ethical codes, and want to ensure that confidentiality of individually identifiable health data is not in jeopardy upon release from hospital records. Indeed, those charged with the safekeeping of hospital health records feel themselves in a quandary. The situation was most cogently expressed in a joint brief by the Ontario Health Record Association and the Ontario College of Health Records Administrators:

Control of confidentiality of medical information is lost once the information is submitted to a centralized agency (corporation), and the data is then subject to leakage as it is readily identified by the OHIP number. This occurs in fact, due to the insistence of the Ministry of Health that the information going to this agency bear the OHIP number and that hospitals submit data to this centralized medical record corporation. The logical conclusion



is that the government itself is grossly breaching patient's rights by demanding that complete information from all hospital medical records be transmitted to the Hospital Medical Records Institute and is therefore readily available for the Government's use. The public is not generally aware of this practice nor is it generally aware of the further ramifications, i.e.; that this information is vulnerable to linkage and leakage beyond the Ministry of Health.

Additionally, The Public Hospitals Act does not permit the release of information from a hospital medical record to a centralized computer agency despite the Ministry's policy to the contrary. This then, is an example of secondary use of information given in good faith by the patient and released without his knowledge or specific authorization.

As I have already observed, legislation relating to hospital medical records does not provide for the release of information to HMRI, or to any other data processing agency. Section 48(1) of Regulation 729 provides that:

Subject to subsections 2, 3, 4 and 5, a board shall not permit any person to remove, inspect or receive information from a medical record.

None of the subsections referred to has any application to this issue. From the evidence at our policy hearings it can be inferred that the Ministry of Health takes the position that, notwithstanding the language of section 48(1), the release of information by hospitals to HMRI is not a breach of the Regulation because,

...the hospitals are allowed to process their patient records in the manner that they consider to be appropriate, using a third party. In fact, it is a fairly well established pattern in North America. A number of hospitals have used, prior to the use of the HMRI, American agencies such as PAS.

I am unable to accept this explanation. There seems to me to be a need to amend The Public Hospitals Act to clarify the responsibilities of hospitals and of the service agency with respect to the very private personal information that is in their care. I endorse a recommendation made by the Ontario Health Record Association in its brief:

*Recommendation:*

43. That The Public Hospitals Act or a regulation made thereunder, or any successor legislation to the Act that may be passed, expressly authorize the practice of releasing patient information to the Hospital Medical Records Institute for data processing.

Currently, HMRI's service is set out in a contract between the Minister of Health and HMRI, with the hospitals as third party beneficiaries. The most recent contract is dated April, 1978. While the contract contains a number of commendable provisions, for the purpose of authorizing and validating the practice, it is an inadequate substitute for legislation, particularly in the light of the existing statutory provisions.

The 1978 contract contains some sound provisions relating to the confidentiality of data:

8.1 Subject to anything to the contrary to this Agreement, HMRI will at all times, both before and after the expiry or termination of this Agreement, preserve absolute secrecy with respect to any data in the Ontario Data File and, without limiting the generality of the foregoing, will

- (a) take all such precautions and measures as may be necessary to ensure that no person has access to any such data other than for the purpose of enabling HMRI to perform its obligations under this Agreement; and
- (b) not make any copies of any document, tape or other thing containing data from the Ontario Data File, except to the extent necessary for HMRI to perform its obligations under this Agreement.

Other provisions deal with agreements with subcontractors:

6.3 Where, by virtue of HMRI subcontracting out any part of its operations, the subcontractor might obtain possession of any document, tape or thing containing data from the Ontario Data File, HMRI will

- (a) ensure that the contract contains covenants by the subcontractor
  - (i) to return any such document, tape or other thing to HMRI as soon as it has served the purpose of enabling the subcontractor to perform his obligations under his contract with HMRI;
  - (ii) to preserve absolute secrecy with respect to any such data and to take all such precautions as may be necessary to ensure that no employee of the subcontractor and no other person has access to any such data other than for the purpose of enabling the subcontractor to perform his obligations under his contract with HMRI;
  - (iii) to not make any copy of any document, tape or other thing containing data from the Ontario Data File, except to the extent necessary for the subcontractor to perform his obligations under his contract with HMRI; and
- (b) take all such measures as may be necessary to retrieve any document, tape or other thing referred to above in the event the subcontractor does not return the same to HMRI forthwith after it has served the purpose of enabling the subcontractor to perform his obligations under his contract with HMRI.

In response to a questionnaire on security of computer systems to the Ministry of Health, Management Systems Branch (then known as Systems Management and Co-ordination Branch, or

SMAC) we received this account of data flow from the director, David E. Harry:

#### HMRI DATA PREPARATION, OUTPUT, AND PROCESSING

The Production Control section of HMRI is responsible for the control and processing of HMRI Abstract data and for distribution of all reporting. The Production Control area of HMRI is used for storage of Abstract documents, for key-verification, and for all handling of input documents and output reports. This area is closed to all unauthorized personnel.

HMRI data is transported in sealed packages or, if within the Metropolitan Toronto area, by one of the following courier services.

- Gauley-Gage Cartage Ltd.
- Hospital Purchasing Incorporated
- Purolator Courier Ltd.

The Abstract documents are stored in the Production Control area at HMRI for 3 months after processing by the computer.

Then they are logged out and incinerated by the Metropolitan Toronto Department of Works-Refuse Disposal Division under the supervision of an HMRI employee.

#### INPUT PREPARATION

HMRI Abstract forms are prepared by the Hospital's medical records personnel from the medical chart of each hospital patient discharged. These Abstracts are batched and, together with a control document, are shipped in sealed envelopes to HMRI via mail or courier. At HMRI, the documents are received by the Production Control area, checked, logged and stored.

#### PROCESSING

Thrice weekly, stored Abstracts documents are logged out, placed in sealed packages and sent via courier to IBM for OCR scanning (data capture). While at IBM data security is observed as outlined in IBM DATA CENTRE

SERVICE AGREEMENT #R-55-6272. All Abstracts, data tapes and listings are placed in sealed packages and returned to HMRI via courier. At HMRI they are checked and logged back in. The Abstract forms are stored in the HMRI Production Control area. The captured data is key-verified and placed on magnetic tape.

These magnetic tapes and their content are logged, a Run Request form is prepared and then they are sent via courier to the Ministry of Government Services - Leaside Data Centre for computer processing.

There, the Data Control section at Leaside Data Centre checks the tapes against the Run Request document and sends them to the tape library where they are kept for 15 days after processing and then erased.

Data Control (Leaside) prepares and submits the computer job which processes the data. After use, tapes are held in the Leaside Data Centre Tape Library until their retention period expires once the job has been run. [emphasis added]

Data Control (Leaside) verifies a successful run by examining the job Control printout and Program Control logs. Output reports are despoiled. All output is placed in sealed packages and returned to HMRI via courier.

#### Distribution of Output

At HMRI, the Production Control personnel verify the processing using the Program Control logs and the Run Control report. All reports are checked, split up, placed in sealed packages, and sent via mail or courier to the hospitals.

The retention period mentioned in the underlined clause refers to the tapes, not to the data per se. The monthly data are in due course transferred to an annual master, which has archival status.



The contract between HMRI and the Minister of Health does not specify retention schedules for documents or tapes. In practice, HMRI appears to dispose of abstracts and working tapes with suitable dispatch. The abstracts are burned when a truck-load has accumulated (about every three months), under the supervision of an HMRI employee. IBM scanner tapes are recycled as soon as an edited tape has been successfully processed. However, I am not aware that there is any time limit with respect to the retention of data on the HMRI file. The following clause in the contract appears to limit HMRI's retention of data, but there is, in practice, no such limitation. It is stipulated that HMRI:

8.1(b) not make any copies of any document, tape or other thing containing data from the Ontario Data File, except to the extent necessary for HMRI to perform its obligations under this Agreement.

In addition to providing reports to hospitals, HMRI is required

2.1(d) at the request of any hospital, [to] provide to the hospital the data in the Ontario Data File which originated in the hospital;

Since hospitals may continue to request material from the HMRI file indefinitely, HMRI is under no obligation to destroy old data; in fact, it may be under an obligation not to. It seems reasonable to place a modest time limit on retention of data with HMRI, based on the most common needs of hospitals. Unusual needs for data at a later date could surely be satisfied through the Ministry of Health which maintains the same file and has better reasons for storage over a longer term.

By the contract, HMRI is permitted to re-release data to researchers:

8.2 Notwithstanding paragraph 8.1, HMRI may disclose data to persons engaged in health care research, provided that

(a) HMRI has first investigated and satisfied itself as to the merits of the research project and the integrity of the persons engaged therein; and

(b) in any event, no data will be disclosed which might identify, or permit any

person receiving such data to identify, any recipient or (unless the provider consents to such identification) any provider of health care services.

At our hearings, C.R. Coleman, executive director of HMRI, described the procedures for responding to researchers' requests:

Q. Is there a committee that is set up that evaluates [the release of information for research purposes], or how is it handled?

A. It depends on the detail of the information that is required. If it is Ontario-wide data which doesn't identify a hospital, doesn't identify a physician number, does not identify a patient number, then I can release it by arrangement with the board. If hospital identifiable data is required, I have to write to those hospitals and obtain their permission before I release that data. If, and it hasn't happened yet, even more breakdown is required, they want to get a doctor number or a patient number, then the hospital would have to obtain the physician's and/or patient's permission before I could make that available.

One example of a purely statistical request that was answered was that of the Ministry of the Solicitor General for the total number of gunshot wounds recorded across the Province over a given period of time.

Section 48(5)(f) of Regulation 729 authorizes the Ministry of Health to receive information from medical records:

A board may permit,

. . . . .

the Director of the Research and Planning Branch or the Department or his authorized representative approved by the Commission or an officer or employee of the Commission who is designated by the Chairman,

to inspect and receive information from a medical record and to be given copies therefrom.

For our purposes, one may substitute the word Ministry for the word Commission. Subsection (6) circumscribes the Ministry's power to re-release data:

Any information received under clause (f) of subsection 5 shall not be used or disclosed to any person for any purpose other than the purposes of compiling statistics and carrying out medical and epidemiological research for or approved by the Department and the Commission. [emphasis added]

Again, for the words Department and the Commission, one may substitute the word Ministry. The underlined provision makes the Ministry responsible for approving re-release of data; there is no indication that the responsibility may be delegated outside the Ministry. Yet in paragraph 8.2(a) of the contract between HMRI and the Minister, HMRI is given the right to evaluate research projects and the integrity of researchers.

Hospitals can use the reports sent to them by HMRI for such purposes as planning and management, medical audit, accreditation and research. Information about actual, as opposed to potential, use is not available. The Ministry of Health is completing a study of actual utilization of reports by hospitals; the report is expected in June, 1980. The Hospital Data Committee Report on the Ministry of Health Individual In-Patient Reporting System for Hospitals, 1977, reported:

Despite the potential, only a few hospitals appear to take reasonable advantage of HMRI output. In summary:

- most large teaching hospitals make routine use of all HMRI tables for teaching, medical audit and administrator purposes.

- the larger hospitals make use of the index reports - procedure, diagnosis and physician.

- most hospitals make use of the hospital summary report. A number hold that this item alone is worth the total HMRI cost

since manual methods are tedious and labour consuming.

- physicians and surgeons in smaller hospitals do not use HMRI tables. This is probably due to limited resources within the hospital to explain the system and educate the practitioners in its use, coupled with a general lack of interest.

Under-utilization of HMRI reports by hospitals is worth mentioning because of the significant effect this has on the quality of HMRI data. Appendix C of the Hospital Data Committee Report is "A Study of Data Quality of the 106 and H.M.R.I. Systems." This study found that

...7.9% and perhaps a much higher percentage, of HMRI diagnoses are incorrect.

The study found that hospital attitudes towards HMRI were a major factor:

...the quality of medical data received via HMRI is primarily dependent on how carefully hospitals individually choose to adhere to HMRI coding guidelines. Hospitals' adherence to proper coding is in turn largely a function of the importance that HMRI data have for their own internal operations. In short, hospitals submit HMRI medical data of whatever quality they see fit, and to the extent that such data are of good quality, it is perhaps only because these data are useful for hospitals' own purposes.

This situation carries important implications for Ministry applications of HMRI data, because of the questionable value of the data for statistical reports and research.

Hospitals were, of course, required to use HMRI as of 1974, though not all of them accepted the need for the service. There has been a major indirect benefit from the exclusive use of HMRI for hospital data processing of this type in Ontario, and that is that the health data now stay within this province's jurisdiction. Before the Ministry of Health made it mandatory for almost all Ontario hospitals to subscribe to HMRI, some hospitals had been using a similar data processing service based in the United States, namely Professional Activities Study (PAS) of Ann Arbor, Michigan. PAS is still used by many hospitals in

other provinces. Although I have no reason to criticize PAS in its handling of health data from Canada, the fact remains that an American company is not accountable to a Canadian jurisdiction, even though part of its data base pertains to Canadian residents. At present, it is not possible to set or control standards of data protection beyond our borders. There are indications of increasing concern about the flow of information across international borders. In 1979, a conference was held in New York on "Data Regulation: European and Third World Realities". A report on this conference by Phil Hirsch of Datamation magazine included comments by a representative of the Canadian government:

Peter Robinson, chairman of the Canadian government's computer communications secretariat, reported that his country's imports of computing services will total \$300 to \$350 million in 1978. The "major point" is that "by 1985, Canada will have annual imports of about \$1.5 billion worth of computing services," he added, and therefore, "it is quite unlikely a Canadian cabinet will decide in favour of an entirely unregulated (international information flow) regime."

. . . . .

Although "economic chauvinism" is a major reason for disagreement over the need for data protection regulations, it isn't the only one. This came out during a question and answer session following Robinson's presentation, when a member of the audience -- Richard Harris, of Xerox -- asked whether Canada would tolerate processing of its data in the United States if carried out "according to Canada's wishes, without loss of earnings." Robinson's answer, in brief, was "no." Reason: Canada "wants to retain control and is willing to pay extra" if necessary to retain this control. [emphasis added]

We do not know for all hospitals how HMRI reports are handled internally. During our hearings, we heard about the procedures at University Hospital, London, from Suzanne Vorvis, its co-ordinator of medical records and, incidentally, a director of HMRI:



...we are a research facility so we do have a large number of research projects that we process through our department. When we receive a project and it is agreed upon that it is appropriate to carry through this project, we will pull data from those printouts. For instance, if a doctor wished to do a study on a certain group of patients, we would be able to pull from our printout only those patients with that particular disease entity or procedure. So we use our printouts for that. We do not give, at this time we are not releasing any of the printouts to physicians. We do not send them copies of the reports. We have one physician who does want to know how many procedures, what procedures he did as a main procedure in the year, every year he wants to know annually and what we do is we obtain our information from our printout then type it up separately and give him that.

Q. Are those printouts utilized by the medical review committee?

A. The printouts themselves are not reviewed by anyone but my department. For which probably I have been criticized, but the medical record committee obtains information that has been taken from the printout. The audit committee obtains information that has been taken from the printouts. Statistics are submitted to the board, as well as to administration occasionally from those printouts, but not directly.

At University Hospital, HMRI output is treated with strong regard for confidentiality of data. I am unable to tell how typical the procedures described by Mrs. Vorvis are among hospitals generally.

There is a need to define the status of HMRI printouts with relation to the hospital medical record. The identifiability of patients from the printouts varies from report to report. The Chart Number Listing provides easy access to information if a patient's chart number is known. This particular report summarizes almost all information from each patient's abstract in chart number sequence. It is at the hospital level that the

chart number is vulnerable to matching with the patient's name, so that this index must clearly be accorded a high level of security. Some printouts, such as Length of Stay reports, carry only statistical data and are far less sensitive.

*Recommendation:*

44. *That printouts received by hospitals from the Hospital Medical Records Institute containing individually identifiable material be subject to the same confidentiality, security and access provisions to which hospital medical records are subject. In the case of purely statistical reports, less restrictive access may be justifiable, so long as information about individuals cannot be identified even indirectly.*

The Ministry of Health HMRI file is found in the Data Development and Evaluation Branch of the Information Systems Division. The actual uses made of the data by the Ministry may be inferred from the provision in paragraph 14.1 of the contract with HMRI:

14.1 Where the Minister proposes to use data derived from the Ontario Data File for any purpose other than epidemiological analysis and research, facilities and services planning, resource utilization and allocation, Program evaluation or management of health care costs, the Ministry will consult with HMRI prior to implementing the analysis of the data.

As I have already pointed out, in 1978, the HMRI file was linked to the OHIP 106 file to create the H/6 file. The linkage was implemented upon the recommendation of the Hospital Data Committee, which was set up by the Data Development and Evaluation Branch of the Ministry,

...to develop recommendations for resolving the role of HMRI in the Ministry information systems.

With respect to linkage, the Committee's task was

...an examination of...the linkage criteria necessary to facilitate integration of

systems and to permit acquisition of individual health-related data on non-OHIP files.

Although much of the Report deals with the potential value to OHIP of the linkage with HMRI data, the prime motivation for the linkage appears to have been the incorporation of names from the 106 records with the health information in the HMRI records. HMRI data are not now used in the insurance process.

Both the H/6 and HMRI files are used to derive statistics in aggregated form for various types of users: hospitals, District Health Councils, Ministry of Health, other government users, and researchers. In a sense, the Ministry is in competition with HMRI in that hospitals may request statistics from either HMRI or the Ministry. The H/6 files are being linked with Health Service Organization (HSO) rosters to identify hospital utilization by roster members. (HSOs are multiservice community health centres.) The Minister has agreed to pass on to The Ontario Cancer Treatment and Research Foundation the H/6 records of all patients with cancer diagnoses.

Representations made to me indicate concern on the part of health-care providers regarding inclusion of patients' names in government health data files. The Ministry of Health has in the past been sensitive to protestations after requesting personal material in individually identifiable form. In its brief, the Ontario Division of the Canadian Mental Health Association (Mental Health/Ontario) described such an occurrence:

On June 13, 1974 the staff of Queen Street, Mental Health Centre circulated a petition objecting to the proposed system of Out Patient Registration which would have required the institution to provide the Ministry of Health with information which in the staff's opinion was unnecessary. The petition read as follows:

We, the undersigned, object to the proposed system of completing an Outpatient Registration form on each outpatient.

We also object to the inclusion of each outpatient's name on the form entitled Patient Services, which records what services are provided to which patients.

We object on the grounds that this information will be used to form a central registry of persons labelled as psychiatric patients under treatment or having received treatment.

We fail to see how such a system will be of any benefit to our patients. On the contrary this system seems to represent a violation of their right of consent to release of information, their right to privacy and anonymity as persons receiving psychiatric treatment as well as the ethical requirements of confidentiality of all professions in treating their clients.

We believe that this information, once supplied, is out of our control, and even if an airtight system of control is presently available, we cannot predict future changes in government policies which might vary the ways in which the information is utilized.

Finally, given our outpatient population, we see this as prejudicial to persons of lower socio-economic status.

On August 27, 1974, the Joint Advisory Committee at Queen Street Mental Health Centre passed a resolution requiring staff to code patient names on the Outpatient Registration Forms and retain the code within the Centre. In addition, a resolution was passed recommending the Ministry of Health not implement the Outpatient Registration System until its legal and ethical implications has been explored.

The incident illustrated staff concerns about disclosing information to a data bank when the rationale for collecting the data did not justify the breadth of data requested. In this case the name of the patient was unnecessary.

The Queen Street Mental Health Centre, as one of the psychiatric hospitals directly administered by the Ministry of Health, does

not report on its patients to the HMRI system. However, as noted earlier, private psychiatric hospitals are now required to report on their in-patients, as are psychiatric units of general hospitals. As a result of the creation of the H/6 file in 1978, therefore, psychiatric information about in-patients of these institutions is recorded, along with the names of the patients and various numerical identifiers.

The inclusion of the OHIP number on HMRI abstracts has long been opposed by a number of hospitals, some of which refuse to supply this piece of information. The following submission is found in the Ontario Hospital Association's brief:

Neither the OHIP number nor the S.I.N. are germane or necessary to the function of HMRI processing records data to assist hospital medical staffs in auditing clinical care. In the opinion of the Ontario Hospital Association the collection of such identifying data threatens the privacy of the patient and it should not be included on HMRI forms. The Ontario Hospital Association has previously been successful in urging that the Social Insurance Number be removed from the form but Ministry of Health representatives have stated their intention that the OHIP number of each patient shall remain on the form.

It appears that the Ministry of Health recognized the validity of these concerns with respect to a data file on therapeutic abortions. The Ontario Hospital Association included this incident in its brief:

In the early 1970's, officials within the Ministry of Health Information System Division of the Statistics Branch issued a form on which was printed at the top:

This information is collected under the authority of the Statistics Act 1971-1972 and subject to the secrecy requirements of Chapter 15, Section 16. Also in accordance with subsection 5 (a) and (b) of Section 251, The Criminal Code (Canada) and RSC 1970, Chapter C-34.

This form was part of RS-61 (rev. 2-9/71) requiring hospitals to provide monthly



reports of certificates issued and therapeutic abortions performed....It originated at the Ontario Hospital Services Commission and its use was carried on after the Commission was integrated into the Ministry of Health. The detailed information required included the OHIP number and the hospital patient register number.

The Ontario Hospital Association recommended that the OHIP number be removed, and a new form without personal identification is now in use.... [emphasis added]

Abortion data reported through HMRI are now stored in the H/6 file along with the OHIP number, patient's name and other identifiers. Jean Base, of the Ontario Health Record Association, made the point that the OHIP number is being used for purposes that go beyond its original intended use.

The OHIP number was invented for the financial arrangements between the hospital and the Ministry, and so information goes in for financial arrangements with the OHIP number. We submit detailed data to the, on an abstract to the Hospital Medical Records Institute and they want the OHIP number on that and the Ministry gets all that information. So there is a potential linkage there between those two files, by using the OHIP number.

It is ironic that the OHIP 106 file has now been linked with the HMRI file by using as the link element, not the OHIP number, but rather a combination of three other data items: hospital number, register number and date of admission. Clearly, the absence of a unique personal identifier does not prevent linkage.

There is continuing concern that the Social Insurance Number (SIN) will be used as a unique personal identifier, increasing the feasibility of linkage with various data files, including some outside the health field. James Hepburn, Executive Director of York Central Hospital, said at our hearings:

Ministry of Health, there's federal, provincial, the vital statistics...we get so much information requested and the big problem is

to make sure that you don't get the social insurance numbers involved where patients could be identified. They do studies on... well, abortion is always a topic that they are trying to get information on. We've got to be very careful how we provide this information, or first thing you know, someone is going to be able to relate two things to an individual person. [emphasis added]

The possibility remains that the SIN might become required information on the HMRI abstract (as it was for a short period when the Ministry of Health first became involved with HMRI). The HMRI abstract still carries a nine-space field in case the SIN is re-introduced. In Attachment "C" of the contract between HMRI and the Minister of Health, provision is made for the implementation of a unique identifier:

These data shall also contain complete patient identification as supplied by the hospital in respect of OHIP number, birth-date, and sex, together with any unique individual identifier such as the Ministry may require hospitals to supply in the future.

The Ministry of Health's position on maintaining a file of individually identifiable health data for hospital in-patients is very different from that expressed by the Ontario Medical Association in its brief:

In providing statistical information to government agencies, other institutions or researchers, every effort should be made to protect the anonymity of patients. Data released should not carry any patient identification, although the origin of the information may be kept on file at the originating hospital. [emphasis added]

. . . . .

The O.M.A. appreciates the need for data collection for statistical purposes. We are supportive of the investigative work being done by the research community towards the understanding and control of various disease processes and in the field of epidemiology. However, we believe strongly that the

information needs in these areas can and must be met through the use of medical records without patient identifiers. Society has more to lose through breach of confidentiality than it has to gain from potential enhancement of research if patient records transmitted and stored for statistical purposes retain patient identifiers.

I am persuaded that there is no good reason for retaining the OHIP number in the data file maintained by HMRI. The number has never been needed by hospital users of HMRI data. With the linking of HMRI records and 106 records by the Ministry there seems to be no need to have the OHIP number on the HMRI abstract. The number is not used as a primary link element, and, in any event, the number is recorded in the 106 records, so that it can be incorporated in the H/6 file. If it is decided that HMRI records at the Ministry should continue to be stored with the OHIP number, then it would be preferable to achieve this by linkage, so that it would be unnecessary for the OHIP number to be involved in the many stages of HMRI processing. Similarly, with respect to patients' names in the H/6 file, it would be preferable to obtain them as a result of linkage with the 106 records (as is now the case), since this procedure would make it unnecessary to have patients' names on HMRI records during processing.

After the creation of this inquiry, a working party was set up within the Ministry of Health to make recommendations regarding confidentiality of health records. A summary of the working party's initial working draft report was made available to me. The Ministry's willingness to review and improve procedures to promote confidentiality of health records in its care is commendable. Two of the problems noted in the working party's report are particularly relevant to the HMRI file. One of these problems concerns

...the definition of the objectives for various areas or bits of information for the Ministry, in order that an information system can be developed on the basis of Ministry needs and obligations rather than an open-ended and undefined information flow.

The draft report recommends:

That the Health Information Review Committee expand their activities to define the

objectives for Ministry information in order that information collection be limited to only those items that serve defined Ministry objectives and meet defined Ministry "needs."

If health information is to be kept in individually identifiable form by the Ministry of Health, no information should be kept that is not demonstrably useful for defined Ministry objectives. The criterion should be the actual utilization of information. If, for example, information is collected for medical research, then it must be evident that such use can be made, and is being made, of the data. Vague prospects of future uses for data should not be considered justification for keeping information stored indefinitely.

According to the evidence I have had, some of the data stored in the HMRI file are not likely to be useful. Much of the data optionally recorded by hospitals cannot even be decoded by the Ministry of Health. Some kinds of optional data can be decoded but since many hospitals do not choose to report particular items it would be impossible to use these for statistics. One example is the data item pertaining to complication rate for surgery. The records of therapeutic abortions would be incomplete because this procedure is often done on an out-patient basis, with the result that the information on file is of limited value. The data from the Alcoholism and Addiction Research Foundation are not required to be sent to the Ministry, a fact that indicates there is not a clear intention to use the data. Particularly in the case of sensitive information, such as abortion and addiction data, there should not be unnecessary storing of information in identifiable form.

Another problem relating to the HMRI file mentioned in the working party's report is that of data retention:

Part of the problem of confidential information is that such information is retained in parts of the medical Records and parts of the Information Systems, long after the need to maintain that part of the information for management or other purposes.

There seems to be no consistent guidelines, administrative or legislative, for destruction or purging of such information either in whole or on a selective basis.

The Ministry has HMRI data dating back to January, 1976, and H/6 data back to October, 1978. No retention schedule had been drawn up for either file as of April, 1980.



## The Medical Information Bureau, Inc.

The Medical Information Bureau should be familiar to anyone who has purchased life insurance in Ontario. When applying for life insurance policies, applicants are required to sign a form of authorization similar to that used by The Excelsior Life Insurance Company which I set out as an example:

### MEDICAL INFORMATION BUREAU NOTIFICATION

One of The Excelsior Life Insurance Company's objectives is to provide insurance at low cost. The underwriting process (evaluation of risks) is necessary to assure this low cost and to ensure that each policyholder contributes his fair share of the cost. In considering your application information from various sources including a medical examination, if required, any reports we may receive from Doctors and hospitals who have attended you, and personal or credit information must be considered.

Information regarding your insurability will be treated as confidential. We may, however, make a brief report thereon to the Medical Information Bureau, a non-profit membership organization of life insurance companies, which operates an information exchange on behalf of its members. If you apply to another Bureau-member company for life or health coverage or a claim for benefits is submitted to such company, the Bureau upon request will supply such company with the information it may have in its files.

The purpose of the Bureau is to protect its members and their policyholders from bearing the expense created by those who would conceal facts relevant to their insurability. Information furnished by the Bureau may

alert the insurer to the possible need for further investigation, but under Bureau rules cannot be used as the basis for evaluating risks. The Bureau is not a repository of medical reports from hospitals and physicians and information in the Bureau files does not reveal whether applications for insurance are accepted, rated or declined.

Upon receipt of a request from you the Bureau will arrange disclosure of any information it may have on your file (medical information will be disclosed only to the attending physician). If you question the accuracy of information in the Bureau's file you may contact the Bureau and seek a correction. The address of the Bureau's information office is:

Medical Information Bureau  
330 University Avenue  
Suite 403  
Toronto, Ontario  
M5G 1R7  
Telephone Number: (416) 863-0518

We may also release information on our file to other life insurance companies to whom you may apply for life or health insurance or to whom a claim for benefits may be submitted.

Have you read the above description?

Yes \_\_\_\_\_ No \_\_\_\_\_

and

#### CONSUMER REPORT CONSENT

I understand that a consumer report containing personal information or credit information may be referred to in connection with my application.

I hereby authorize any licensed physician, medical practitioner, hospital, clinic or other medical or medically related facility,

insurance company, the Medical Information Bureau or other organization, institution or person that has any records or knowledge of me or my health or my insurability to give to The Excelsior Life Insurance Company such information. A photographic copy of this authorization shall be as valid as the original.

Dated at \_\_\_\_\_,  
this \_\_\_\_\_ day of \_\_\_\_\_, 19\_\_.

\_\_\_\_\_  
Witness

\_\_\_\_\_  
Signature

Although, as an American corporation, MIB, Inc. could not be required to attend our hearings, I am happy to be able to say that it co-operated fully in this inquiry whenever asked to do so and sent a well informed representative to our hearings.

As the form quoted above explains, MIB, Inc. is an organization through which member insurance companies exchange health information about applicants for life insurance. MIB, Inc., as it is now known, is a non-profit corporation whose principal offices are in Greenwich, Connecticut. At the present time the company's computer facilities are located in Boston, Massachusetts. There are two disclosure offices, one in Boston and the other in Toronto. The organization was founded by the medical directors of life insurance companies in 1890 to prevent fraud by applicants. Mr. William Swarts, its Associate General Counsel, and the corporation's representative at our hearings, gave this explanation of its origin:

Around 1902, it was reorganized and became part of the Association of Life Insurance Medical Directors of America and was operated as a function of that association. In 1947, it became a separate, unincorporated entity managed independently of the Medical Directors Association, and until 1978, the date of incorporation, was an unincorporated association of member companies.

The certificate of incorporation sets out the purposes of the corporation in the following language:

1. To provide for the exchange on a non-profit basis among the Corporation's member life insurance companies of

underwriting information with respect to proposed insureds and insurance claimants in such a manner as may best protect the accuracy and confidential nature of the information so exchanged and the interests with respect thereto of such proposed insureds, claimants and insurers concerned;

2. to aid its members in their consideration, assessment and assignment of prospective insurance risks by making available information which is essential to careful underwriting practices and procedures;
3. to help prevent perpetration of fraud upon its members and their policyholders by proposed insureds and claimants who may omit or seek to conceal facts essential to accurate, proper and reasonable determination of insurance risk;
4. to assist in mortality, morbidity and related studies of value to life insurers and of benefit to the medical profession and general public; and
5. to engage in any lawful act or activity for which corporations may be organized under the General Corporation Law of Delaware, subject to the restrictions contained in other Articles of this Certificate of Incorporation and the Corporation's Bylaws, and provided, however, that the Corporation is not organized for profit and no part of the net earnings of the Corporation shall inure to the benefit of any member or individual, and that the Corporation shall exercise only such powers as are consistent with the exempt status of organizations described in Section 501(c)(6) of the Internal Revenue Code, and the regulations thereunder, as the same now exist or as they may be hereafter amended from time to time.

The corporation's by-laws contain the following provisions with respect to membership:

Eligibility. Any insurance company of the United States or Canada conducting the business of life insurance on the legal reserve plan shall be eligible provided:

- (a) It shall be duly licensed by and in good standing with the insurance supervisory official of the jurisdiction of its domicile and wherever else it does business, including all places where it sells or delivers policies, whether by mail or otherwise, and whether or not authorized to do business there.
- (b) Its medical affairs shall be administered by a medical director who is a qualified physician in good repute at its domicile, or if its Home Office be in a different jurisdiction from its domicile, then in the jurisdiction in which its Home Office is located.
- (c) It shall pledge itself to maintain the confidential character of the information exchanged and to respect the privacy of the individuals to whom such information pertains and shall also pledge itself to comply with the rules and regulations of the Corporation as adopted by the board of directors.
- (d) It shall agree upon termination of its membership to dispose of any physical property or information received through or because of its membership in the Corporation in such manner as it may then be directed by the board of directors, whether by transfer to a member, destruction, return to the Corporation or another person, or otherwise.

Of its 700 member companies, 80 are Canadian. As of 1977, there were a total of 10,766,424 reports on individuals on file with MIB, Inc., of which 689,000 related to Canadians. Of the 2,685,804 new reports submitted in 1977, 166,765 came from Canadian companies.



Reports are filed with MIB, Inc. by the medical director of the life insurance company to which the applicant has applied for insurance. Although reports may be submitted if the applicant's medical history is normal, the usual practice is that a report is not submitted unless there is a significant medical history such as a heart condition or previous illness. It is estimated that reports are filed with respect to 10 to 20 per cent of all applicants for life insurance.

The member life insurance company must obtain the applicant's consent to the furnishing of information to MIB, Inc. As Mr. Swarts explained,

The authorization is one half of the company's advising its applicant of MIB's involvement in the underwriting picture. The company is also, by our rules, required to give a form of pre-notice, a written pre-notice, which describes MIB and its operations, advises the applicant of the availability of disclosure and disputed accuracy proceedings. So that the applicant knows that he can determine whether or not he has an MIB record and what's in it.

The consent and pre-notice are generally part of all life insurance applications in Ontario. Reports are filed on a special form which includes name, date of birth, birth place, geographic location of last residence and sometimes occupation. The diagnostic information is given as one of 200 codes from the MIB, Inc. code book known as the Official Code List of Impairments. The code list is distributed to member companies only and is the responsibility of the medical director of every company. Copies of the code list are not available at the computer centre or disclosure offices. MIB, Inc.'s general rules stipulate that medical information reported must be given to the insurance company by the applicant, a physician or other health-care providers. Health information from non-medical sources, such as investigation companies, cannot be reported. According to Mr. Swarts, MIB, Inc.'s rules also prohibit reporting underwriting information or decisions. He explained:

...every company has its own underwriting policies and an individual who may not be acceptable to one company as a risk may be very acceptable to another company as a risk. So there is no need to advise, nor have members ever been advised, to my

knowledge, of what action the reporting company took.

The coded forms are mailed to the computer centre in Boston and entered onto the computer. If there is a previous report on an applicant it is brought up to date. Reports, filed by name and birthdate, are kept on the computer for seven years plus one day. Information older than that is purged quarterly.

Member companies obtain access to the information held by MIB, Inc., by sending written requests to the MIB, Inc. disclosure office or by using a computer terminal on the company premises which is linked by telephone to the computer in Boston.

The MIB, Inc. rules specify that, with respect to the placement and use of computer terminals by member companies, every company must file a plan for the approval of the president and operations staff of MIB, Inc. All terminals must have a call-back feature to prevent unauthorized access. An explanation of the procedure was given by Mr. Swarts and can be summarized as follows:

The operator dials the computer centre. The computers connect through a handshaking technique. The computer verifies that it is a proper terminal and company before the actual link-up occurs.

MIB receives the request for information. The computers then disconnect. The terminal does not wait for a reply.

The computer will then reply by retrieving the telephone number in its system, and dialing the company back. The connection is made and the handshaking technique is repeated. Information is then transmitted to the company. The computers disconnect. The information goes to MIB over a different line than it is received on. To their knowledge there has never been a security violation of terminal communication. Nor have there been any complaints over access or other incidents.

While the terminals may be used for other transactions they may not be used to send information to a credit reporting agency. Furthermore, they may not be used to receive information from a credit reporting agency unless the information is favourable to the applicant. When a member company requests information from MIB, Inc. it receives only the MIB, Inc. code and the date the report was received by MIB, Inc., but not the names of the company that filed the report. According to Mr. Swarts, the

purpose of the information is to confirm information already received from the applicant and possibly his or her physician. As to the use made of the information received from MIB, Inc., Mr. Swarts had this to say in the following exchange with Mr. Strosberg:

A. The general rule is that the company cannot make an underwriting decision on the basis of those codes received. They have got to confirm them somehow and they may confirm them through their own medical exam, or they may confirm them through other sources. So they do not have a file that is simply the MIB record. They have the record plus documentation confirming that.

Q. They may have, just have an application from the prospective policyholder himself and take that in conjunction with the MIB if it's a very small policy. I understand that it only costs twenty-five cents a request, is that correct?

A. That's roughly right.

Q. All right. So that if it's a very small policy it may be that they don't want to go to the expense of paying a physician thirty dollars to do a report of an examination?

A. Well, if you were to get an application in and there is that part where the applicant talks about his medical history and you have got an MIB report and the two squared off absolutely, well...

Q. You may not go any further?

A. You may not go any further because you have got a truthful applicant.

Q. Mister Swarts, that's the point I am trying to make.

A. But you have the application and then you have the MIB report and they don't square off, then certainly you are going to want to be able to develop the reasons for the discrepancy, which means that you are

going to have more in your file than the little three digit numbers.

Q. I think what you mean to say, sir, is that at that point a judgment has to be made. An insurance company has to decide whether or not, based on that policy, they are going to take that extra step. I think that's really what you want to say?

A. Well I won't go on further to say that they may be very foolish if they didn't.

If the company to which a person has applied for life insurance cannot confirm the information received from MIB, Inc. it may notify MIB, Inc. that verification is not possible and may ask for further details. MIB, Inc. relays the request for details to the company that filed the report, which company, at its discretion, may provide more details to the inquiring company directly or may, through MIB, Inc., refuse to provide further information. MIB, Inc.'s general rules restrict the number of requests for details a company may make to 15 per cent of the reports requested. These rules also restrict the uses which may be made of the computer terminals. MIB, Inc. has established procedures to monitor the compliance of its member companies with its general rules. Mr. Swarts explained the procedures at our hearing:

There are two procedures. There is a program which we call the company visit program. It is conducted by the Greenwich office. There is a director of the program and five visit consultants, all of whom are retired underwriting executives, one of whom is a Canadian and who has primary responsibility for Canadian companies. This program has been very successful. It started out with a consultant and now with the five consultants and director we are able to visit each company once every two years. A typical company visit would consist of a review of no less than twenty underwriting files which have been selected by our office with a bias. That is to say, there had to be a match up of the applicant and the record. It had to be as current a request as is possible to review. We hope to be reviewing files that are six months old.

Secondly, it must have concerned a report which contained a kind of code that would certainly call the operation of many of our rules into play. These files are reviewed for rule compliance.

Another aspect of the visit of course is to discuss any questions the company might have about MIB rules or new regulations or developments at MIB. Another aspect would be surveying the physical security of the underwriting operation, the terminals, the distribution of code books and so forth. Then this is reported back to our office and our director will advise that company of where possible non-compliance was found and suggest ways that it can be avoided in the future. Or suggest, just suggest procedures that might tend to minimize the kind of expectable human error in any operation which means there is an occasional lapse.

MIB, Inc. permits an individual to have access to his or her own information. The concerned person files a request form at one of the two disclosure offices. The Internal Procedural Rules makes the following provision with respect to a request for disclosure:

1. Upon request and proper identification as hereinafter prescribed (in paragraphs 4 to 8), M.I.B. will clearly and accurately disclose to the applicant:
  - (a) the nature, substance and source (i.e., the name of the reporting member company) of all nonmedical information in its files on the applicant at the time of the request;
  - (b) the source (i.e., the name of the reporting member company) of all medical information in its files on the applicant at the time of the request;
  - (c) the recipients of any M.I.B. report on the applicant which it has furnished within the six-month period preceding the request; except that no sources or recipients will be disclosed with



respect to information received or M.I.B. reports furnished prior to April 25, 1971, except to the extent that the matter involved is contained in the files of M.I.B. on that date.

2. With respect to medical information in its files, upon receipt of a written request of the applicant containing a release from any and all claims and liability which may arise therefrom signed by the applicant, M.I.B. will request the reporting company to disclose the nature and substance of the results of its medical examinations to the applicant's personal physician.

3. Where the member company's report of medical information has been based on information received from an attending physician, hospital or clinic, then the Medical Director of the reporting company will take reasonable action to see that the applicant's current attending physician is advised of the source of information and, if ethical, its contents.

At the hearing, a typical disclosure letter was made an exhibit and formed the basis of the following discussion between Mr. Strosberg and Mr. Swarts:

Q. Look at the letter to Mr. Glen R., Winnipeg, Manitoba, dated May 16, 1978, the second paragraph: "We have a coded report of non-medical information submitted by the London Life Insurance Company, dated 14 July, 1975, which means height, five foot nine inches; weight, two hundred and five pounds; suspected, questionable or doubtful." What does that mean?

A. That the company itself wasn't able, the company which reported it wasn't able to confirm that that was...

Q. Confirm the weight? Or the height?

A. Yes.

Q. They thought he might have been fatter or thinner?

A. He might be fatter or thinner. It may, I do not know the background of this case.

Q. I understand that. It's just an example. All right, let's go on to the next paragraph...

A. In other words, it's a warning to whoever receives this report that the information itself without any knowledge of the source and so on, the information itself may be somewhat questionable.

A. You know, it's an alert to the receiving company to double check this. Don't take this information for granted.

Q. I'm five foot nine and I would like to think of myself as two hundred and five pounds, so I understand what that means very well. "Although this information appears to be medical in nature, it is being disclosed to you because it was not obtained from a physician or other medical facility. We also have medical information pertaining to you and in the near future your personal physician should hear from the following company who reported medical information to the MIB."

Then it gives the name of the company. Now I'm sorry, I may have misunderstood what you said just a few moments earlier, but I thought you said that if MIB had medical information and it comes from a non-medical source that it is given to the person as indicated here?

Mr. Swarts also gave an explanation of the practice of releasing medical information to the individual's physician rather than to the individual himself or herself:

Well, it is a matter of preference with the medical profession, at least in the U.S., that this kind of information be disclosed through a physician who can exercise his

kind of professional judgment on how best to disclose medical information to his patient. We think, we think our system makes sense because the company has only reported to us a code, which is a very non-descriptive, generality if you will. That code is based upon the documentary evidence that the company has in its underwriting file. It may very well be that as the system works the company would say to the applicant's attending physician, we have reported to MIB codes which mean X, Y. That may not even be enough of a disclosure for the physician to be able to relate on to his patient. The reporting company may then choose to amplify our basic requirement, i.e., providing the code translation, with some of the documentation in its underwriting file so that the physician has a fuller understanding that he can pass on to his patient.

. . . . .

I am not saying that the person will misinterpret it or not understand it. I am saying that the preferred procedure today appears to be that this kind of information is best disclosed through a professional, and again I will make reference back to our privacy commission in the U.S., which cast this into its recommendations, this kind of procedure. It is also, it has also been the procedure recommended on proposed amendments to the Fair Credit Reporting Act. I am not going to judge on whether or not it is a good or bad procedure. It appears today to be an acceptable procedure and of course part of what you are doing is defining what is today acceptable or not, and finding out that things that occurred, practices that were general in years past today are not acceptable, but were then. I am not going to say that five years from now the procedures we employ today are going to be acceptable down the line. But we feel that today, within the framework of what we are going through, the method we have chosen for disclosure is the most acceptable. We have had very little complaint about that from

the individuals to whom the information pertains. We have very little complaint from physicians about this because of the extra time this procedure costs them in terms of sitting down with the applicant, who doesn't need treatment at that point. He is not in as a patient, but in to find out what the record was and we have no complaints from insurance companies that we are putting an extra burden on them by making them contact the attending physician.

So we believe that this is an acceptable procedure and is generally accepted as such.

. . . . .

Well, first of all, I hope I am not going to repeat myself too much. There is presently no legal requirement to disclose the medical information. That means if we choose, as we have, to go further than the law's requirements, we can pick the procedure that we feel is satisfactory to all parties concerned because there has from time to time been alarm raised at disclosing information directly to the applicant that for reasons best known to a doctor, for example, he hasn't advised the applicant directly about. I cannot speculate on what we might do if say the medical profession were to feel that direct disclosure was advisable, and I don't know whether or not the medical profession would ever reach that position. It is true that this is not the simplest way that it could be done, but we do believe it is the most effective and acceptable way to disclose this highly sensitive information within the framework that we operate in today.

The insurance company must disclose to the inquiring applicant's physician the meaning of the codes and, by writing to MIB, Inc., confirm that the disclosure has been made.

According to the evidence, approximately six requests for information are received per year from government agencies including the police. In most cases, what is being sought is an

address of a suspect. MIB, Inc. will tell the police whether or not it is in possession of a record but will not disclose any further information voluntarily. I presume the information furnished will support an application for a search warrant or service of a subpoena.

I have heard of no complaint or concern with respect to the security of the data held by MIB, Inc. What was the subject of several submissions and letters was the question whether persons should, in effect, be required to consent to the disclosure of sensitive information to MIB, Inc. as a condition of obtaining life insurance. Of secondary concern was the fact that the information about Canadians is sent and stored in the United States and is thus beyond the reach and protection of Canadian law. Mr. Swarts discussed the requirement that applicants for insurance must consent to the forwarding of information to MIB, Inc. in the following exchange at the hearing:

Q. Do you know whether member companies in effect require the signing of the consent as a condition precedent to really considering a risk?

A. It is difficult for me to speak of general companies' practices because of course each member company is going to exercise different kinds of policies. I would suspect, however, that, as a matter of good business, if an applicant denied the company the right to go to sources of information which are absolutely necessary for them to underwrite a policy, that they would be just as happy not to consider the policy any further.

MR. COMMISSIONER: So what you are saying is, there really is no choice. If they want life insurance, they have to sign the consent? As a practical matter?

A. MIB is only a part, is only one of the information sources listed on that authorization form. The authorization form also speaks to the company's ability to go to the applicant's doctor for information. To go to hospitals and other health facilities. To perhaps contact other life insurance companies if they feel that would be



necessary in order to fully develop the necessary information to underwrite.

. . . . .

A. ...as a matter of business judgment I believe that they would feel that they are not getting the kind of protection that is necessary for them to exercise their responsibilities vis-a-vis their other policyholders and that they would be inclined to decline that particular risk.

Although I question how genuine a consent given or extracted in this way is in fact, I do not believe that the propriety and justification for the practice fall within my terms of reference.

With respect to the "off-shore" storage of information about residents of Ontario, reference may be usefully made to the statement by the Honourable Frank Drea, Minister of Consumer and Commercial Relations, in the Legislature on April 11, 1980, on the subject of the security of data. On that occasion he announced that adherence to "Right to Privacy Guidelines", promulgated by the Canadian Life Insurance Association, would be a condition of licensing of all life and accident insurers. The guidelines are as follows:

#### RIGHT TO PRIVACY GUIDELINES

The nature of the business of insurance as carried out by ABC Life requires that the company collect, use and retain personal information about those individuals to and through whom the company's services are provided and to disclose such information to third parties when authorized or required by law.

The company must balance carefully its need for such information against the individual's right to privacy, the need for fairness, and the need to minimize the intrusiveness, and take necessary precautions to protect these interests.

To that end, ABC Life will be guided by the following guidelines:

1. Only proper and authorized means will be employed to collect that personal information which is pertinent to the effective conduct of the company's business, and to the extent practicable;
  - a) such personal information will be obtained directly from the individual concerned; and
  - b) prior to collection such personal information from any other source, the individual concerned will be notified or the individual's authorization will be secured; and
  - c) pretext interviews and false and misleading practices will be avoided.
2. The individual will be advised, on proper written request, of the intended use of the requested information.
3. An individual, upon proper identification and written inquiry, will be advised, subject to any applicable legal or ethical prohibition or privilege, of the nature and source of personal information about him retained in the company's records. Personal medical information will be made available through the individual's designated physician.
4. Personal information that is collected and retained will be considered to be confidential and proper safeguards will be provided to protect that confidentiality.
5. Every reasonable effort will be made to ensure that personal information collected, used, retained or disclosed is accurate, relevant, timely and complete. An individual may correct or clarify personal information regarding that individual retained by the company.
6. Without the individual's express written consent, the company will not permit access to, or disclosure of personal information

retained by the company to any person, other than an employee or agent with a legitimate business need for the information, except as may be required by legal process, statutory authority, contractual obligation or business practice.

7. All employees, agents, brokers and other persons or organizations acting for or on the company's behalf will be required to conform to the applicable guidelines.

While the guidelines do not, of course, directly apply to MIB, Inc., insurance companies should ensure that any other agency storing data provided by them comply with the guidelines. It should be the responsibility of the insurance companies to see that all information is stored in a facility, wherever it may be located, that complies with the guidelines that must be observed in Ontario, and to withdraw information from any facility whose standards are not at least as high. With respect to the Ontario guidelines set out above, I need not repeat here what I have said elsewhere in this report about the practice of making information available to a person about his or her health only through his or her physician and not directly. Nor will I repeat my comments on the subject of the obtaining of health information by means of pretexts. In that connection paragraph 1.c) of the Ontario guidelines should be strengthened to express the principle that "pretext interviews and false and misleading practices will be prohibited." Finally, one can say with confidence that, at the present time, any suggestion that MIB, Inc.'s standards are not as high as those in the Ontario guidelines is without justification.

## Hospitals and Other Health-Care Institutions

In the course of discharging their principal responsibility of providing care and treatment, hospitals become holders and distributors of a very large amount of patient health information. In the performance of their primary function as health-care providers hospitals are outstanding; their secondary function of protecting the confidentiality of the health information of their patients is one which, according to the evidence we have had, is often not carried out as carefully. The result is that many persons and organizations frequently have access to information about hospital patients and former patients without the permission of those patients or without any other legal authorization, with the consequence that the privacy of those persons is violated.

With the creation of this inquiry and the media's coverage of our investigation of various practices relating to breaches of hospital patients' privacy, these institutions have begun to pay more attention to their duty as guardians of confidential patient information. Indeed, some hospitals have embraced this role with such fervour that the proper flow of information for permitted purposes has been unfortunately affected. Hospitals urgently require a clarification of their responsibilities and guidance in carrying them out.

An appropriate place to begin a discussion of the confidentiality of patient health records in hospitals is with the legislation which now governs these establishments and their records, since this is the origin of many of the problems which currently threaten the privacy of hospital patients. Hospitals in Ontario are categorized for purposes of legislation according to the type of services they provide, their ownership and operation, their affiliation with a university, and the type of patient they admit. Hospital legislation and statutes respecting other institutional health-care providers are not primarily concerned with the protection of patients' confidential health information. The provisions for the safekeeping of medical records and the privacy of patients in hospitals and these other institutions are found in various statutes and regulations. The existing legislation and regulations are detailed in the patient record comparison charts and accompanying text in the summary of

Ontario Legislation, found elsewhere in this report. The major problem areas are described here.

Most of the hospitals with which I am concerned are public hospitals and are regulated by The Public Hospitals Act, R.S.O. 1970, chapter 378. Regulation 726 under this Act classifies the following types of public hospitals:

...general hospitals, convalescent hospitals, hospitals for chronic patients, active treatment teaching psychiatric hospitals, active treatment hospitals for alcoholism and drug addiction and regional rehabilitation hospitals...

There are over 240 of these public hospitals in Ontario. According to section 11 of The Public Hospitals Act, the medical record of the public hospital patient "is the property of the hospital and shall be kept in the custody of the administrator." Regulation 729 (as amended by O. Reg. 353/71, section 2) under this Act requires that a medical record be compiled for each public hospital patient, and sets out the components of the medical record in detail in section 38(1):

The board shall cause to be compiled for each patient a medical record including,

- (a) identification;
- (b) history of present illness;
- (c) history of previous illnesses;
- (d) family history;
- (e) provisional diagnosis;
- (f) orders for treatment;
- (g) progress notes;
- (h) reports of,
  - (i) condition on discharge,
  - (ii) consultations,
  - (iii) follow-up care,



- (iv) laboratory examinations,
- (v) medical, surgical and obstetrical treatment, including renal dialysis treatment,
- (vi) operations and anaesthesia,
- (vii) physical examinations,
- (viii) radiological examinations, and
- (ix) post mortem examination, if any;
- (i) final diagnosis; and
- (j) death certificate.

Section 48 of the Regulation permits the disclosure of information from this medical record to certain persons under certain circumstances. By section 39, the superintendent of the hospital is given responsibility for the safekeeping of all patient records; in sections 42-47a a complex record retention schedule is set out, with the duty of ensuring that the medical records are properly destroyed being assigned to the hospital administrator.

Approximately one quarter of the public hospitals contain psychiatric units "for the observation, care and treatment of persons suffering from mental disorder", and therefore are also designated as "psychiatric facilities" under Regulation 576 under The Mental Health Act, R.S.O. 1970, chapter 269, as amended by S.O. 1978, chapter 50. Under section 26a of The Mental Health Act, a patient's record is called a "clinical record", the composition of which is not defined. Subsection (1)(a) of section 26a says that:

"clinical record" means the clinical record compiled in a psychiatric facility in respect of a patient, and includes a part of a clinical record;

This general definition, as contrasted with the itemized, physician-recorded components of the medical record in Regulation 729 under The Public Hospitals Act has led such bodies as the Ontario Hospital Association to conclude that the composition of the clinical record is not "confined to medical information recorded by a physician." The question whether or

not the clinical record is meant to be different from the medical record required to be compiled for all patients in public hospitals is one which arose during the hearing attended by the Ontario chapter of the Canadian Mental Health Association (Mental Health/Ontario):

MR. COMMISSIONER: Can you shed any light on what the clinical record is as opposed to the medical record, which is the phrase used in The Public Hospitals Act, which may have a psychiatric facility?

MR. BAKER [Counsel for Mental Health/Ontario]: Yes. I think there is a definition for clinical record in here that makes it clear that it is the intention of the legislation that there be two records kept in the general hospital setting, the medical record and the psychiatric record, which is the clinical record that is referred to here.

I am not certain that the clinical record compiled in a psychiatric unit of a public hospital should be interpreted as a document that is distinct from the medical record, but the point is that, under the present legislation, the matter is far from clear.

Section 26a of The Mental Health Act identifies persons who may be permitted to have access, under certain conditions, to the clinical record or parts thereof. These recipients and the circumstances under which the disclosure of the clinical record may occur under section 26a are different from the recipients and conditions required for disclosure of information from a public hospital medical record under section 48 of Regulation 729. This means that, within the same public hospital, the access to and the release of the health record of a psychiatric patient is governed by different considerations from those regulating the disclosure of the information from, for example, a cardiac patient's record. If the cardiac patient was having difficulty adjusting to his illness and visited the hospital's "psychiatric unit" for observation, care and treatment, the disclosure of his or her health information would, it seems, be governed by two inconsistent release provisions.

Unlike The Public Hospitals Act, The Mental Health Act does not contain provisions for the ownership, safekeeping, storage or destruction of the clinical record. It is possible that the provisions of The Public Hospitals Act and Regulation 729

relating to the security of the medical record also apply to the clinical record in public hospitals designated as psychiatric facilities under The Mental Health Act, section 3 of which provides:

Every psychiatric facility has power to carry on its undertaking as authorized by any Act, but, where the provisions of any Act conflict with the provisions of this Act or the regulations, the provisions of this Act and the regulations prevail.

On the other hand, if the clinical record is indeed a distinct and separate document from the medical record, (as the clinical record contains information not recorded by a physician, and Regulation 729 specifies that under ordinary circumstances, "nurses' notes...and other notes not made by a physician...are not part of the medical record") it may be that the clinical record is not to be maintained in the same way as the medical record.

Another type of hospital which is designated as a psychiatric facility under The Mental Health Act is the provincial psychiatric hospital. Regulation 578 under The Mental Hospitals Act, R.S.O. 1970, chapter 270, designates 11 hospitals in Ontario as psychiatric hospitals, although one of them, the Lakeshore Psychiatric Hospital has recently been closed. They include hospitals with such varying degrees of physical security as the Penetanguishene Mental Health Centre, the St. Thomas Psychiatric Hospital and the Queen Street Mental Health Centre in Toronto. The definition of a patient's "clinical record" and the provisions for its examination and release found in section 26a of The Mental Health Act govern the patient information maintained by these psychiatric hospitals. The absence, in The Mental Health Act, of any provisions for the ownership, safekeeping, retention or destruction of the clinical records in a psychiatric facility has already been pointed out. The Mental Hospitals Act also contains no provisions regulating these matters. Section 4 of The Mental Hospitals Act authorizes the Lieutenant Governor in Council to "designate any provision of The Public Hospitals Act or of the regulations thereunder as being applicable to any institution under [The Mental Hospitals Act]", but no such designation has been made.

Yet another type of health-care institution in Ontario is the community psychiatric hospital. Regulation 94 under The Community Psychiatric Hospitals Act, R.S.O. 1970, chapter 74, contains only very general safekeeping, maintenance and internal distribution provisions, although the itemized medical record

is almost as detailed as that of the public hospital record. However, all five community psychiatric hospitals are designated psychiatric facilities under The Mental Health Act; four are also designated public hospitals under The Public Hospitals Act; and the fifth is also a children's mental health centre governed by The Children's Mental Health Centres Act, 1978, S.O. 1978, chapter 67, which statute is administered by the Ministry of Community and Social Services.

The network of Acts and regulations relating to confidentiality of patient information in Ontario health-care establishments is further complicated by still more legislative categorization. Nineteen health-care facilities are governed by The Private Hospitals Act, R.S.O. 1970, chapter 361. Although section 10 of Regulation 689 under this Act makes the superintendent responsible for the safekeeping of all patient records, there are no provisions relating to private hospital record confidentiality, disclosure, retention or disposal. Private hospitals cannot rely on any of the sections of The Public Hospitals Act relating to patient records, since section 2 of this Act says:

Nothing in this Act in any way relates to or affects a private hospital under The Private Hospitals Act.

However, two private hospitals are also psychiatric facilities under The Mental Health Act.

Nursing homes for extended skilled nursing care are governed by The Nursing Homes Act, 1972, S.O. 1972, chapter 11. Regulation 196/72 under the Act sets out medical and drug records confidentiality, inspection, disclosure and retention provisions which are similar to, but not nearly as extensive as, those pertaining to public hospital records. In contrast, the records of residents in nursing homes and approved homes licensed under The Homes for Special Care Act, R.S.O. 1970, chapter 205, are not protected by that legislation. Section 35(a) of Regulation 438 under this Act requires "a detailed report on the medical history of the resident before admission and all physical and mental examinations...after admission" to be kept by the administrator, but there are no provisions for confidentiality, disclosure, retention or disposal of the record.

Apart from the institutions regulated by provincial legislation, there are at least 18 health-care facilities operated by the Federal government in Ontario, including nursing stations, medical centres and general hospitals serving the native Indian

and Inuit population as well as other northern Ontarians. The confidentiality of the patient information in these Federal health-care establishments is currently not provided for in any legislation. Another hospital which is not governed by legislation respecting confidentiality is the Workmen's Compensation Hospital and Rehabilitation Centre at Downsview, which is under the jurisdiction of the Workmen's Compensation Board.

I am not the first person to direct attention to the absence of any systematic legislative approach to the confidentiality of records in institutions in Ontario. The Ministry of Health's Working Party on the Confidentiality of Health Records had this to say about the state of affairs in 1978:

There are numerous inconsistencies between the various Acts and Regulations under the Acts in particular those related to Institutions (The Public Hospitals Act, The Mental Hospitals Act, The Mental Health Act, The Community Psychiatric Hospitals Act, etc.) with regard to legal and administrative procedures for the safe-keeping of the Medical Record in order to maintain confidentiality of information. Such inconsistencies include procedures with regard to consent, to the definition of responsibility for maintenance of the Record, to the rights of access by different individuals to the Medical Record or portions of it, and the Legislative provisions under which access to the Record, for clinical use or for research, is allowed....Only in the Amendment to The Mental Health Act is there instruction with regard to deletion of patient identification from a Medical Record, before access is allowed, as well as allowance for access to only a defined part of the Record rather than blanket provision for access.

In the existing legislative scheme only The Mental Health Act itself is the location of the relevant provisions; in other cases one must search the regulations. It is not unfair to say, then, that the legislative scheme relating to the confidentiality of medical records lacks consistency and clarity and is not easily accessible. Generally speaking, this, in essence, was the complaint of such concerned groups as the Ontario Hospital Association, the Patients' Rights Association, Mental Health/Ontario, the ad hoc committee of the Department of



Psychiatry at the University of Toronto, the County of York Law Association, the Ottawa General Hospital, and the Ontario Health Record Association.

Improvement is urgently needed. The proposal of one statute to govern and protect the confidentiality of records in any type of hospital, institution or health-care facility was made to me many times during the course of the inquiry and is something which several American jurisdictions, such as Connecticut and Maryland, have already carried out. Another example of such an omnibus Act is the U.S. Bill H.R. 5935, the "Federal Privacy of Medical Information Act", described as "a bill to protect the privacy of medical information maintained by medical care facilities" which I have referred to elsewhere in this report, and to which I shall make further reference to below.

Uniform provisions governing health records should extend beyond such institutions as public, private and psychiatric hospitals, to include all health-care facilities. Licensed or approved homes for the aged, homes for special care, nursing homes, developmental centres, rehabilitation centres, specialized clinics, home-care programmes and community health agencies are not hospitals but all offer care for persons and maintain health records for this purpose. These facilities, and any others which are legally empowered to offer medical or health-related care to patients, ought to meet the same standards of confidentiality.

#### *Recommendation:*

45. *That all facilities or institutions legally empowered to provide health-care services and maintaining patient records be regulated by the same or similar provisions governing the confidentiality of patient information.*

A recommendation for uniform legislation means, of course, that the present 'double standard' of privacy for psychiatric and non-psychiatric records (as evidenced by the discrepancies between section 26a of The Mental Health Act and Regulation 729 under The Public Hospitals Act) would be replaced by one uniform standard of confidentiality for all types of information maintained in health-care facilities. This is worth pointing out because support for the continuation of a different standard of confidentiality for psychiatric patient information was shown by various persons and organizations who made submissions during the inquiry and is reflected in practices in other jurisdictions. Those who support the application of a different

standard of privacy for psychiatric patient information argue that the stigma that attaches to those suffering from mental disorders makes their medical records more sensitive than those of non-psychiatric patients, since any disclosure of their mental problems could be extremely unpleasant and even hazardous for the psychiatric patient. Such a view was expressed in the Ministry of Health's booklet, Rights and Responsibilities, published to clarify the 1978 changes in The Mental Health Act:

The rules, until now, have not provided sufficient protection for psychiatric records. In a public hospital, for example, no distinction is made between psychiatric-patient records and others. While the improper release of information dealing with a surgical patient's broken leg may cause the patient little harm, to reveal details of the history and diagnosis of a psychiatric patient could not only cause the person serious psychological harm, it could well jeopardize the person's entire treatment program.

As a matter of policy I am not persuaded of the validity of this distinction. The Ontario Medical Association made this observation in its brief:

...records are not so easily divided into psychiatric and non-psychiatric categories, nor are all psychiatric records or all psychiatric patients located in psychiatric hospitals. The mixing of patients in public general hospitals and the existence of psychiatric illness with physical illness make it imperative that all medical records be treated with the confidentiality necessary for psychiatric records.

A demand for a higher standard of privacy protection for psychiatric information gives rise to an inference that a lower standard of confidentiality is acceptable for non-psychiatric health records. In my opinion, in an enlightened society, no support ought to be given to a distinction that suggests that mental illness carries with it a social stigma. The development of policy should be encouraged that would eliminate any stigma that may, in fact, exist. No prejudice results from this approach because it does not involve a lower standard of care for psychiatric information. It simply has the effect of enhancing the protection given to other sorts of health information by

raising the level to that appropriate for psychiatric information. To repeat, what is needed is one high standard of confidentiality for hospital patient records regardless of the nature of the information. I accept the submission in the brief submitted by the Ontario division of the Canadian Mental Health Association:

One legal standard should govern confidentiality of both psychiatric and non-psychiatric records.

This can be provided by uniform legislation to preserve the confidentiality of all types of health information in all types of health-care facilities.

By way of background for specific proposals for legislative change, an introduction to hospital administrative procedures and the problems affecting the confidentiality of their patients' health information would be helpful. To this end I shall describe the typical departments of an Ontario hospital, to make clear what patient information each department generates or contains, how it maintains it, and what risks there are to its confidentiality. Since every hospital is different in size, service and patient population no "average" hospital exists in fact. The policies and practices to be described are based primarily on information provided by the public hospitals, but are, in my opinion, characteristic of Ontario health-care facilities in general.

When a patient enters a hospital for observation, tests, diagnosis and treatment, extensive personal, health-related material is generated about him or her and circulated within the hospital. The flow and proliferation of patient information begin with the information collected upon admission of a new patient, gain momentum as reports are created by the various parts of the hospital involved with the patient, and continue even after the patient is discharged, and his or her record travels on to the hospital's medical record department, the only department in the hospital the principal function of which is to maintain patient records. I shall examine the amount of patient information held by other departments, the number of persons who have access to this information, how long it is retained, how securely it is stored, and what eventually becomes of it, as well as the unauthorized flow of information out of the hospital.

## The Admitting Department

Admission is the formal reception and acceptance of the patient by the hospital and may be initiated through either the admitting or the emergency department. An out-patient is a person who is received in a hospital for examination or treatment or both, but who is not admitted as a patient. A patient is defined in section 1(1) of The Public Hospitals Act as "a person received and lodged in a hospital for the purpose of treatment." In common parlance a "patient", as opposed to an "out-patient", is referred to as an "in-patient".

Upon admission, a hospital admission report form supplied by the Ontario Health Insurance Plan and termed a "form 106A", or simply "a 106A", is completed for the patient. The revised (August 1979) version of this document contains space for the following information about the patient:

Hospital Number  
\*Patient's Surname, First name  
Patient ID Number  
\*Register Number  
\*Admission Date, Time  
\*OHIP Number  
\*Ambulance  
\*Language  
\*Relationship to Subscriber  
\*Responsible for Payment  
\*Birthdate  
\*Sex  
Marital Status  
Previous Patient  
Alternate Name or Previous Name  
\*Age Group  
\*Residence Code  
Type of Admission  
Address, Postal Code  
Phone  
Religion  
In Emergency Notify--Name,  
(Relation), Address, Phone  
OHIP Group--Name and Address  
Responsibility for Payment & Other Insurance  
Data  
Accommodation: Required, Assigned, Room  
No., Rate  
Transferred From  
Family Physician  
Referring Physician

Attending Physician  
Admitting Diagnosis  
Signature of Patient or Guarantor (assuming  
responsibility for charges not paid by  
another agency)  
Other Data

Only the information denoted by an asterisk is actually required by OHIP; the use of the remainder of the form is at the option of the hospital. The standard 106A form package includes one copy for the hospital and one OHIP claim copy, but a hectograph continuous carbon set is also available to the hospital for further duplication. (It should be noted that this OHIP form is not used by the 11 provincial psychiatric hospitals all of which have their own forms for admission and discharge.)

The hospital and OHIP copies of the 106A are sent to the hospital's accounting department so that it may begin the OHIP accounting process. While still in the admitting department, duplicates of this OHIP form are generated for distribution to other departments within the hospital. One or two copies are usually sent to the following departments or individuals: the physician or physicians involved in the patient's care, the medical record department, the business office (to be made into a patient account ledger card), the main information desk (to answer inquiries from the public), and the social service department. At least one copy remains in the admitting department. The Toronto General Hospital finds that in order to fulfill its internal hospital distribution requirements, it must copy the entire OHIP 106A form and the more limited "public information" sections of this form a combined total of 20 times for each patient admitted to hospital.

The more copies of his or her personal and health-related information that are circulated and the more hospital personnel who have access to this information, the less privacy the patient has within the hospital. However, the flow of information within the hospital gains real significance and becomes a cause for concern when it facilitates a communication of information from the hospital to the outside world, as the investigation of the private investigators' activities has illustrated.

There is a further dissemination of admission information within the hospital, but this is usually by means of a shortened version of the information on the 106A form, often termed "public information", "social information" or "non-confidential information" by hospitals. The hospital switchboard, minor information desks, department of pastoral care, the post office, and the patient's ward or floor may, and normally do, receive



the following information, largely for the purposes of answering inquiries by the public:

Patient's: Name  
Address  
Sex  
Religion  
Room Number  
Physician's Name

Often this is supplemented by more personal information, such as the patient's occupation, phone number, age, next-of-kin, referring physician and date of admission. However, the explicitly medical information on form 106A, that is, the admitting or provisional diagnosis, is not considered a part of this "public information".

Even this so-called non-confidential or public information which hospitals use to answer outside inquiries about individual patients is private information to some patients, as in the case of the psychiatric or obstetric patient who does not want even the fact of his or her admission to hospital disclosed to anyone. Consequently, there is reason to question the broad circulation of admission and "public" information throughout the hospital, and whether every department I have mentioned has a justifiable "need to know" the amount and type of personal information which it often automatically receives from the admitting department.

The following exchange at our policy hearings attended by representatives of the Ontario Hospital Association illustrates the problem:

MR. COMMISSIONER: Is there, for example--I think maybe the answer to this is yes, now that I think about it--is there a daily list that is circulated among a certain number of people in the hospital of admissions for that day?

MISS MORAN: Yes.

DR. GALLOWAY: Very definitely.

MR. COMMISSIONER: With a diagnosis on it?

MR. SLUTE: Yes. A presumptive diagnosis, yes.

MR. COMMISSIONER: Yes. Is the distribution--I can understand that the kitchen has to know, but what is the--is there a careful decision made about the distribution of such information?

DR. GALLOWAY: There should be, Mister Commissioner. For example your information desk also has to know who has been admitted, but they do not need to know what the admission diagnosis was. If you are a large hospital, the department of pastoral care, for example, they need to know who was admitted. But they don't need to know the admission diagnosis. There are other areas that do need to know that. I think the concern that you are expressing is that first of all I think those documents should be franked confidential and treated as confidential. Secondly, they should not be posted in public areas. They should be handled in the manner that confidential documents should be handled.

I suppose every hospital should periodically examine what distribution has been made, because I think what happens is you start out with a distribution and it keeps getting added to for whatever reason, so I think periodically you have to look and say what distribution is this document receiving, and why are they receiving that.

Two other points may be made before leaving the admitting department. First, the number of staff members employed in the admitting department varies with the size of hospitals, but one can assume that, in a large number of hospitals, a significant number of clerks, typists, and non-professional employees, who are without the guidance of an ethical code dealing with patient confidentiality which membership in a health profession brings, come into contact daily with a substantial amount of patient information. Second, the admitting departments of hospitals retain copies of patients' full 106A forms within their departments for months and even years after the patients have been discharged. From the private investigators' reports which we examined, we learned of a number of incidents in which information from these forms held by admitting departments relating to former patients had been disclosed to private investigators. The threat to a patient's privacy which admission information

may pose remains present long after he or she has passed through the admitting department or, indeed, the hospital.

### The Emergency Department

Many patients enter the hospital through the emergency department, the primary function of which is the reception and treatment of persons in emergency situations. In most hospitals the emergency department maintains a register which identifies the patients treated in the department and when they were treated, which physicians they saw, whether they had laboratory tests, x-rays or a surgical procedure, whether or not they were admitted to hospital, discharged from emergency or died, and what their chart numbers were. Some hospitals include more medical information on their emergency registers, such as the patient's condition and physician's remarks. Because actual medical treatment is given in the department, an individual emergency record or chart is also created for all patients treated there.

During the same hearings I asked three local hospitals, the Windsor Western Hospital Centre, Inc., the Hotel Dieu of St. Joseph's, and the Metropolitan General Hospital to inform me about their procedures for storage and security of emergency department records. Although these are records of medical treatment given to patients in the emergency department, all three hospitals described their emergency room records as being kept in filing cabinet drawers which are unlocked, and are easily accessible to emergency personnel who include clerks, typists, service co-ordinators, clinical co-ordinators, nurses, nursing assistants and physicians. The emergency charts remain within the department for varying periods of time before they are completed and sent to the medical record department for storage. For example, while the Windsor Western Hospital's practice was to retain these records in their emergency room for approximately one month, the Metropolitan General Hospital held them there for a two-month period and the Hotel Dieu Hospital for even longer. It was because of procedures of this sort that a nurse and former employee of the emergency department at Metropolitan General Hospital in Windsor was able to take advantage of the system and supply information from the emergency records to her husband, a partner in a private investigation firm. But other private investigators did not need an 'inside' source in order to receive certain types of patient information from the records of emergency departments in many other Ontario hospitals; their investigation reports show that they could frequently learn from these departments whether their subject had been a former patient of the hospital, whether he or she had

been treated by the emergency department, the dates of treatment, who the subject's physician had been in the hospital, who the family physician was, and, in some cases, what type of injury had been sustained.

For all patients requiring ambulance service to or from the emergency department there is an Ontario Ambulance Services Information System ambulance call report, which contains information about the patient's injuries and condition (including the emergency physician's evaluation of how "essential" the service is). The OASIS ambulance call reports (Form 5), which are completed in quadruplicate, are distributed according to various formulas set out in Schedule 4 of O. Reg. 599/75 under The Ambulance Act, R.S.O. 1970, chapter 20. Distribution depends on the billing source, which may be the hospital of origin, or destination, or the ambulance service performing the call. For example, where the billing source is the destination hospital, Form 5 is to be disposed of thus:

```
Copy 1.    OASIS      )
              )
Copy 2.    Billing    ) deposited at destination hospital.
              )
Copy 3.L.  Update stub)
```

R. Patient--handed to person receiving patient.

Copy 4. Ambulance Service--retained.

In some variations of the formula all four copies are not required. For example, if the destination is non-medical, the patient copy is to be discarded, but the regulation does not specify how that is to be done.

The proliferation of forms containing confidential health information is not the only threat to patient privacy associated with ambulance services. I was told of incidents in which ambulance attendants opened sealed envelopes containing patient information addressed to personnel in the receiving institution. The ambulance drivers examined these patients' records to discover medical conditions which could require special care during the ambulance ride, or, perhaps, a history of violence to which they wanted to be alerted. The ambulance attendant may need to know this type of information about the patient in his ambulance, but, at the moment, his or her right to the information in light of the present provisions of section 48 of Regulation 729 under The Public Hospitals Act is not clear.

## The Ward

The admitted person, now a patient, settles into a ward or unit, the place where most health care occurs and most health information is generated. An active patient chart or medical record is created for every patient to document his or her condition and treatment for the entire course of hospitalization. Earlier in this chapter I set out the contents of this medical record, as prescribed by section 38(1) of Regulation 729, made under The Public Hospitals Act. The sensitive health information which it contains, including the patient's medical history, diagnosis, and reports of his or her examinations and treatment, is extensive. When the patient is discharged from the hospital, this chart is transferred to the medical record department for long term storage and safekeeping.

Upon the patient's entrance to the ward, a nurse completes an "admission to unit" report on the new patient, and begins the "nurses' notes". These are notes made by the on-duty nurses several times a day for the period of hospitalization, recording the general progress of the patient's condition, attitude, behaviour, and reaction to medication. In accordance with the provisions of section 37(1) of Regulation 729 under The Public Hospitals Act, within 72 hours after admission, a physician must write the patient's medical history, make a physical examination, and record the resultant findings with a provisional diagnosis of the patient's condition. The patient's attending physician then records his or her orders for the patient's treatment and the tests to be conducted. "Progress notes" of the patient's condition are also made from time to time by the physicians involved, and these and other physician-created reports are all attached to the patient's chart. If the patient leaves the ward temporarily, perhaps for x-rays or an operation, the reports from these procedures are sent back to the ward and also attached to the patient's chart.

While the patient is in the hospital the active chart is usually retained at or near a nursing station in the patient's ward, and is left unlocked for easy access by the unit staff. At our hearings, Isabel Brown and Maureen Powers of the Registered Nurses' Association of Ontario described the lack of security of the chart in the patient's ward:

MS. BROWN: I think it's a very common experience. If you walk into a nursing unit in many hospitals around this province I think you can challenge that those records are secure. If I walk in there on twelve to eight, there is no nurse sitting in that



nursing station at that time and those records are there for anyone who wishes to walk in and pull it out.

MR. COMMISSIONER: Is that a serious problem? Is it likely? We are not now talking about the medical records department. We are talking about the records for patients who are now in hospital and their records need to be at or near the nursing station closest to their rooms. It is clear that it would be unsatisfactory if you required those records to be in the medical records department so that every time you added to them or had reference to them you had to go to a different part of the hospital. Is it a serious problem that they are in an area which is easily accessible to members of the caring, the treating team?

We have heard in evidence of persons walking into a hospital purporting to have a right of access to the records because of some relationship with the patient, but from your experience is it a problem of some magnitude? That is to say that people do go up to these records who have no right to them?

MS. BROWN: People do walk up to them who have questionable right of access, and I think that if they are familiar with some of the physical settings some of these records are in what we call a pass-through kind of setup where the nursing station is on one side and there is a physicians' recording area on the other side. There is no supervision, or relatively little, supervision of who goes in or out of that section, and anybody can walk in there and with no identification, no need to identify himself, and have access to those records.

MR. COMMISSIONER: Can, you say, and does?

MS. BROWN: Does. If a nurse challenges, there is very great difficulty for her. On what basis is she challenging? Unless she asks for identification, and she does get a card that says so-and-so, she doesn't know

whether that is the attending physician who has the right of access. Some nurses have attempted to do that kind of challenge and have been challenged back and anybody who wants to put on a white coat, which seems to give people some indication that they have a right to be in the situation in the hospital, can go in and take the record and have, apparently, access to it.

MR. COMMISSIONER: So what you are saying, as I understand it, is that it is not uncommon that physicians or residents or interns who have no connection with the patient, for reasons other than the care of the patient, go to these areas, pull the chart out and read them and if the nurse should ask what right that person has, the nurse is treated in something less than a pleasant fashion?

MS. BROWN: She can be. Most of the time she..

MR. COMMISSIONER: I am more interested in real life than possibilities or hypothetical situations. This occurs, I take it, from what you say?

MS. BROWN: It has been reported by some nurses that it has happened. But most of the time they would probably not even challenge.

MR. COMMISSIONER: The nurse wouldn't challenge?

MS. BROWN: Right.

MS. POWERS: Can I say something about that? I think what we are saying in our brief is that records are kept in a variety of places. For example, they are kept in boxes outside client's rooms. They are kept at patients' bedsides, some part of the records are kept at patient's bedside. And in conveyances that are wheeled around the patient's unit. The experience of being involved in this kind of presentation to

this hearing, I think, has enabled us to recognize the sensitivity of these documents. Having been, for instance, in a pediatric environment, I have experienced where parents of one child have read the record of another child, that happened to be available, and found, obtained information about that child's condition. I think that although it is important to have documents available to the health professionals involved in the care, what we as health professionals have to be very cautious about is the availability of those documents to other people.

To keep the charts on the ward easily accessible for patient-care purposes and, at the same time, safe from the curious eyes of unauthorized readers is a problem of physical security that may be different for every hospital. In the discussion of physicians and their clients it was pointed out how a physician without hospital privileges took advantage of the lax security, or trust, on the floor to obtain patient information to which he had no right. The reluctance on the part of receptionists, clerks, and nurses to question the authority of physicians to have access to a patient's information is understandable, given the perceived status of physicians in hospital organization, but it can jeopardize the privacy of the patients. To minimize the jeopardy, the right of employees to protect the charts from unauthorized inspection and to question the right of access on the part of persons not recognized as being entitled to read them must be supported and reinforced. At Victoria Hospital, a teaching hospital in London, the staff are required to carry badges bearing their photographs which they are asked to produce if someone at the nursing station is concerned about the right to inspect a given chart. Although this is a commendable safeguard well worth implementing everywhere, it is, of course, not a complete solution to the problem. A solution that would make impossible the occurrence of a breach of the trust that exists and must exist may be a benefit not justified by the cost.

Subsections 1 and 3 of section 46 of Regulation 729 made under The Public Hospitals Act, when read together, provide that, in ordinary circumstances, nurses' notes, and other notes not made by a physician are not part of the medical record but must, nevertheless, be retained for five years from the date of discharge or death of the patient. The medical record itself eventually arrives at the medical record department which places a high priority on security. If nurses' notes are not part of

the medical record they are not required for the purposes of the medical record department. Nevertheless, they must be retained somewhere for a period of five years. The place of storage actually chosen depends upon the decisions of the individual hospitals. Some hospitals do, in fact, file the nurses' notes with the medical record in the medical record department. Other hospitals, on the other hand, file them separately and treat them differently, usually, we have discovered, with less care than the medical record.

### The Psychiatric Unit

If it is the psychiatric unit of a public hospital to which a patient is admitted, the medical record is developed in much the same way as the non-psychiatric chart, and is retained in the psychiatric ward or floor until after the patient's discharge from hospital. Eventually this inactive record goes to the medical record department, where it is maintained in the same manner as any medical record.

However, a certain amount of patient-identified information remains within the psychiatric department. For example, if a patient is being treated in another part of the hospital and is sent to the psychiatric department for an assessment, a copy of the assessment report remains in the psychiatric department. Moreover, this department often retains records containing material that was omitted from the official medical record because of its unsubstantiated nature. That material may include the physician's own notes containing his suspicions and theories, the impressions and opinions of the social workers, nurses, and other staff members of the psychiatric ward, as well as statements made by the patient's friends, family and neighbours. At one of our hearings, Dr. Peter O'Hara, medical director of Scarborough General Hospital, described his hospital's system of creating an official document for the medical record department while, at the same time, maintaining an unofficial psychiatric record within the department:

We have a system of records where the medical record of the psychiatry patient, the assessment and sort of the evaluation and I guess the treatment of the patient by the psychiatrist, plus the orders he writes, that goes to the medical records room. Now there is another record that is really compiled by public health nurses, social workers, para-psychiatric workers, and this is kept up on the psychiatric floor. A lot

of it is just hearsay. That they have gone out and spoken to people and relatives in the community and they, I don't really think this is part of the medical record.

The Toronto General Hospital keeps the full medical records of its psychiatric out-patients within the psychiatric department, sending an "official file" on each patient, containing minimal identifying information, to the medical record department to be used in case the patient is seen in another part of the hospital, particularly in emergency situations.

### Auxiliary Services

Not all of the hospital's health-related services take place in the patient's ward or unit. Patients often require the services of the hospital's specialized diagnostic and therapeutic departments, such as x-rays by the radiology department, body fluid analyses by the clinical laboratory, body tissue examinations by the pathology department, electro-cardiograms or electroencephalograms by the E.C.G. or E.E.G. departments, blood from haematology, drugs from the pharmacy, physiotherapy from the physical medicine division, occupational therapy from the occupational therapy department, the advice of a social worker from the social service department, or isotopic scans from the nuclear medicine department. It is usual for these departments to maintain their own patient records, thus making for a proliferation of medical reports throughout the hospital.

### The X-ray Department

Section 47(1) of Regulation 729 provides that x-ray films are part of the medical record unless a report of the radiological examination is written by a physician and retained as part of the patient's medical record. In practice, therefore, the x-ray film itself is not attached to the patient's chart which does, however, contain the radiologist's report. The film is retained in the radiology department along with a document containing the patient's identifying information and a copy of the radiologist's report. During one of our investigative hearings an employee of the North York General Hospital's radiology department, when asked what information his department had about a particular patient, gave this description:

We have on our file card, we have their name and their address and their OHIP number, their age, date of birth, the doctor that



saw them, whether they were in-patient or out-patient, however, and going to the films we have the results of the x-ray.

Subsection 2 of section 47 of Regulation 729 requires that x-ray films be retained for as long as five years, but radiology departments do not often have the facilities for maintaining them securely. The staffs of many hospital radiology departments are small. Hotel Dieu of St. Joseph's in Windsor admitted that its department is often left unstaffed. The absence of security in hospital x-ray areas was discussed at our hearings by James Bruce, the associate administrator of North York Branson Hospital, who testified that, prior to September 1971, his hospital kept its patients' recent x-ray films in linear shelving in the corridor near the x-ray department.

The retention of a primary medical document in an insecure area of the hospital, for a required length of time, by technical staff untrained in record maintenance, poses an obvious threat to patients' privacy. Radiology departments have been a fertile source of information for private investigators. Since it is common for physicians to call the radiology department to inquire about the results of x-rays on their patients, the private investigators were frequently able to telephone this department and have a clerk or a technician read out the x-ray results as a matter of course.

### The Laboratory and Pathology Departments

During a patient's stay in hospital his or her health care may require the involvement of the hospital's clinical laboratory and pathology departments. The clinical laboratory tests the patient's body fluids and related matter for the presence of such things as sugar, bacteria, and malignant cells. For an analysis of such specimens as surgically excised bone marrow, body tissue, organs, or the "products of conception" removed during an abortion, a pathology report is requested. The pathology laboratory makes its examination and writes its report, describing any malignancy, inflammation, or other abnormality found in the specimen. Under section 47a of Regulation 729 (as amended by O. Reg. 100/74, section 9), a tissue specimen that has been made into a slide for microscopic examination, must be retained in the hospital for five years, if it discloses a significant abnormality or if the administrator is advised of the existence of litigation in which the slide might be relevant, and for two years if there is no significant abnormality.

As for the written laboratory reports, often several copies are made for the purpose of circulation within the hospital. We learned of the number and wide intra-hospital distribution of copies of the pathology report after some 3,600 copies belonging to The Wellesley Hospital were found blowing across a 12-block area of downtown Toronto on June 12, 1978. These pathology report copies were dispersed when a plastic garbage bag fell from a disposal company's truck at Sherbourne and King Streets into a 30-40 mile-an-hour wind.

The copies of the pathology reports placed in evidence contained information identifying the patients fully, including their home addresses, hospital room numbers, admission data and physicians' names. The medical information they contained was extensive: the pathologists' findings and diagnoses, the requesting physicians' notes and clinical diagnoses. Many of the reports were analyses of abortion, miscarriage or cancerous specimens. The director of environmental services at The Wellesley Hospital, Thomas Kingsborough, testified at our hearings about his hospital's policy for the generating and disseminating of copies of these pathology reports within The Wellesley Hospital and its neighbour, The Princess Margaret Hospital:

I visited Doctor Carruthers at the pathological laboratory, Princess Margaret, from whom it was learned that the distribution of the completed requisitions were: original to the office Central Laboratory for distribution to the patient area concerned for inclusion on the patient's chart, and then the first copy went to Princess Margaret path[ology] office. The second copy went to the attending physician for his information, and the third copy went to medical records.

The extra copy to medical records was in case the original is not in the chart, when it gets back to medical records after the patient is discharged.

These extra copies, made for the medical record department in case the original became misplaced, were involved in the dispersion following the fall from the disposal company's truck, and of the 3,600 extra copies, only 187 at most, or five percent, were ever used by the medical record department.

As Mr. Kingsborough pointed out, one copy of the laboratory report also remains in the pathology department. This is a practice required by section 35a of Regulation 729 (as amended by O. Reg. 100/74 section 6) which says:

- (1) Where a report is made,
  - (a) as the result of a pathological or other laboratory examination of a patient or an out-patient;  
or
  - (b) of any tissue, fluid or other material removed from a patient or an out-patient,

the original report shall be part of the medical record of the patient or out-patient.

(2) A copy of the report made under subsection 1 shall be retained in the laboratory where the examination and report referred to in subsection 1 were made, for three years from the date when the report was made and may be destroyed at any time thereafter by the director of the laboratory.

(3) Notwithstanding section 43, a statutory declaration is not required where a copy of a report is destroyed under subsection 2.

The retention of a copy of a primary medical document in a hospital laboratory for a designated length of time with no guarantee of its full and proper destruction places the confidentiality of this information at risk. The Ontario Hospital Association expressed its disapproval of section 35a through its executive director of Association Services, Roger Slute, during one of our policy hearings:

We have asked the government formally several years ago to remove section 35(a) from the regulation, talking about copies have to be kept of laboratory reports in the laboratory. Now they should be kept there for out-patients who do not have an in-patient medical record. The doctor's

patient outside should get the original, and the lab[oratory] should keep a copy. But inside the hospital, again required by this law, to produce and hang on to for certain lengths of time copies of these things is bad law and we have asked the government to repeal that section 35a. It increases the danger as long as it's there.

The accidental spillage of pathology reports also brought into question the adequacy of hospital procedures for the destruction of confidential patient documents. The Wellesley Hospital had no uniform policy or system to regulate the destruction of the confidential material located throughout the hospital. There was variation between, and even within, departments as to how long documents were retained and how they were destroyed. For the pathology report copies in the medical record department, The Wellesley Hospital had an "informal" system of reviewing the reports every six months and then destroying them. The clerks in charge of the destruction of the pathology reports in question testified that they had been given no written or oral directions on how to dispose of confidential documents. They usually tore the six-months old pathology report copies in half before placing them in the garbage. The reports found blowing around 12 Toronto blocks had not been torn in pieces because the clerks had been pressed for time on the day in question and threw the pathology reports out intact. There was no control mechanism by which proper destruction was monitored.

Ellen Barnes, the hospital's director of medical records testified that in the course of her career she had worked for three other hospitals in various departments, and none of these hospitals had policies or written directives on disposal methods for "day-to-day" departmental records to which the staff could refer. Although the hospital owned a shredder which could have been used to render the copies of the pathology reports completely unidentifiable before destruction, it had not been used. Manu Malkani, assistant administrator of medical services at The Wellesley Hospital, testified that he knew of no reason why this shredder could not have been used on the pathologists' reports, adding that perhaps the two clerks "at the time didn't appreciate the sensitivity of the situation." This lack of awareness by employees of a responsibility to protect the confidentiality of patient information is a critical factor in the inappropriate disclosure of private information. To assume, as Mrs. Barnes did, that her staff would be aware that pathology reports should be torn in a manner that would prevent confidential information from being disclosed, is an unwarranted assumption:

MR. COMMISSIONER: Why would you assume that they knew that the purpose for which they were tearing them up was to protect confidentiality as opposed simply to getting rid of unnecessary material?

A. Anyone working in a medical records department, as far as I am concerned, is and should be aware of the confidentiality of the records and this is why they would be tearing them up.

MR. COMMISSIONER: Well I take it that there--in any given medical records department of a hospital the size of yours--you have people with training from the post-secondary education down to, I suppose, grade school level. Is that correct?

A. Yes.

MR. COMMISSIONER: If you don't have an inhouse course or written set of instructions, how can you assume that persons at any level of employment or any level of training would have the same understanding of the need for confidentiality?

A. I guess I can't assume that.

### The Operating Room

Many patients require surgical procedures and the services of the operating room facilities during their stay. It is necessary for these patients, located in different parts of the hospital, to be organized and prepared for their operations at the right time because of the busy nature of the operating room schedule. This requires the creation of operating room lists. These lists or schedules contain the following information: patient name, operating room number, date and time of operation, operative procedure to be performed, and name of surgeon and anaesthetist.

Operating lists are copied up to 50 times by some large hospitals, before being circulated throughout the hospital to a variety of offices, laboratories and other departments and posted at every nursing station. David McWilliams, Q.C., who represented Metropolitan General and Windsor Western Hospitals



at our Windsor hearings, said that "in many cases the nursing stations are not concerned about 90 per cent of the people on the particular list, and yet it is distributed universally through the hospital...." This common practice not only places confidential information on hospitalized surgery patients before the eyes of many staff members totally uninvolved in the health care of those listed on the schedules, but it also exposes the operating room schedules to members of the public visiting the hospital, as Roger Slute of the Ontario Hospital Association pointed out:

I believe that it has been recognized in some hospitals and I know of one case where a man was coming in to visit his wife and he happened to be going by whatever area and he was stopped from going or prevented from going wherever it was, and he wasn't searching out information, but he saw the bulletin board with the OR schedule and his wife's name, and I don't think it was a therapeutic abortion, and he immediately sort of did an about face and went to the administration and said, I really don't think my wife's confidentiality is worth a hoot if you paste these all over, and it was just something that had been natural, it's necessary for good numbers of people in a hospital to know and plan on a daily basis and they did then examine very carefully where those things were going and how many were being produced. It is a potential problem.

Although these schedules are produced daily, there was no evidence of procedures in place to collect and destroy them after they had served their purpose.

Widespread, uncontrolled circulation, careless security and unorganized destruction practices are completely inappropriate for such sensitive health information, and reflect an inadequate concern for confidentiality. No doubt many employees do require some of the information which the operating room schedule provides, but the evidence indicates that most of them actually need only about 10 per cent of the information they now receive. The relatively small number with a true need to know cannot justify the existing distribution procedures for operating room schedules.

At least one hospital represented at the hearings had given some attention to this problem, however. St. Thomas-Elgin

General Hospital makes more than one list in an attempt to provide the various hospital departments with only as much patient operating room information as they need. The executive director of the hospital, Jon R. Skafel described the practice as follows:

We try to guarantee privacy to all our patients and when the operating room schedule is made up it has to be distributed to quite a few areas in the hospital. The procedure is not put on for anybody, except for the specific places where it is required in order to say prepare the patient for the surgery. That nursing unit, for instance, they may get the schedule. They will have the procedure to be performed for a particular patient because they have to get the patient ready to go to the operating room, but the dietary department, for example, which receives a copy of the operating room schedule for its meal distribution purposes does not know what procedure is being performed. They only know patient X is booked for surgery.

MR. COMMISSIONER: What about the administrative offices?

A. I receive that copy of the full operating room schedule with the procedure on it, but it's a very restricted distribution.

The operating room also generates documents which become part of the patient's medical record. These documents consist of an "information sheet" briefly describing the facts of the surgery, an anaesthesia record setting out the anaesthetic procedure, a recovery room record with graphs of the patient's physical reactions, and the operation record written by the surgeon. It does not appear that copies of these documents remain in the operating room or operating room office, although copies are sent to the offices of the physicians involved.

### Paramedical Services

Hospitals contain various paramedical departments serving both patients and out-patients. They include the social service department (offering the skills of social workers and related personnel), the department of rehabilitation or physical

medicine, sometimes divided into the physiotherapy, speech therapy and occupational therapy departments, and the dietary department. These sections of the hospital each maintain their own patient records, the contents of which vary in accordance with the needs of the services provided.

For the patient whose health is related to social problems and who is referred to the social service department, a record is maintained in that department containing referral information, the patient's identifying data, and notes on the progress made under treatment; if the patient requires long-term treatment his or her record includes a complete social history, an account of the patient's present situation, and full progress reports. The evidence I have seen suggests that hospitals often consider a patient's social information to be less sensitive than his or her medical information and have released the former type of information much more readily to third parties without the patient's consent.

The physiotherapy unit maintains individual records fully identifying the patient, the number, dates and types of treatment provided and usually a primary diagnosis and physiotherapists's assessment. Doreen Yates, secretary and receptionist of the physiotherapy department of York-Finch General Hospital in Downsview, testified that these records are maintained in her department for about three years. We found that the physiotherapy department of many hospitals readily disclosed such information as the number of times a patient received physiotherapy and the dates on which his treatment started and stopped, without the patient's knowledge or permission. This disclosure was especially helpful to private investigators inquiring about the treatment of accident victims.

### The Department of Pastoral Care

Most hospitals offer the services of a resident chaplain to provide counsel and spiritual comfort for their patients. It is a common hospital practice for these members of the clergy to be given the diagnoses of the patients with whom they become involved without first obtaining the patients' permission. I received a number of complaints from hospital employees and administrators who question the propriety of the access of the clergy to confidential information. Others, like James Broderick, assistant executive director of Windsor Western Hospital Centre, Inc., argue that the clergy often play a significant role in the patient's total health care process and are part of the medical team. This is how he put it at our hearings:

A. Yes. At our hospital, we have a resident chaplain, and I think the resident chaplain is considered part of the medical team to the extent that through dealing with the staff, and dealing with the patient, I think they definitely know the diagnosis of many of the patients, especially the serious patients, or the ones they are getting involved in. They do know the diagnosis, and I think it is a matter of record they are there to assist them in the spiritual end.

. . . . .

MR. COMMISSIONER: Does the hospital chaplain, by virtue of his being the hospital chaplain, have access to those patients' records?

A. No sir. He has access to no patient records. The hospital chaplain has no access.

MR. COMMISSIONER: Even where he is acting as pastoral counsel for that patient?

A. Yes sir. He has no access to records.

MR. COMMISSIONER: I thought your answer was he was part of the team?

A. No. He has access to a team conference involving that particular person, and to use an example, a rehabilitation patient, where they have a team conference, and parts of the need of that patient are classified as spiritual needs, and that patient--and therefore if somebody comes out and says "This person has indicated a need for somebody from the clergy to be there", they will discuss that, and maybe our resident chaplain will contact say a priest or minister or rabbi to come in and assist in dealing with that person.

It appears to be the case at some hospitals, however, that clergymen obtain access to patients' charts as a matter of course and without difficulty.

## The Out-Patient Department

A patient who does not require treatment in the emergency department or hospitalization may be cared for by visits to the hospital's out-patient department. It will be recalled that section 1(k) of The Public Hospitals Act defined out-patient as:

...a person who is received in a hospital for examination or treatment or both, but who is not admitted as a patient.

However, an out-patient may be a former patient of the same hospital. A full health record is developed on the condition and treatment of each out-patient seen by the hospital. If an out-patient was a patient of the hospital on a prior occasion, his or her out-patient medical record may be a continuation of his or her patient medical record and not a separate file.

Out-patient medical records are held in the out-patient department in some hospitals; in others they are retained in the medical record department and brought to the out-patient department prior to the patient's appointed visit and returned there after it. In still other cases, individual departments of the hospital, such as the clinical laboratory or the psychiatric department retain their own set of out-patient records. At our investigation hearings it was determined that the out-patient department itself was not often responsible for unauthorized disclosures of patient information.

## Medical Record Department

After the patient is discharged from the hospital, or dies, his or her chart is transferred from the ward to the medical record department, the central repository for inactive patient medical information in the hospital. When it reaches the medical record department, the inactive chart is then checked by this department's staff for any deficiencies and assembled into a formal medical record. A "summary sheet" must be included, listing the patient's operations, diagnosis, complications, and assigning a final diagnosis. The attending physician's "final note", summarizing the patient's medical history, physical examination results, and course of treatment while in hospital must also be included.

Sometimes, however, the chart is not completed or signed by the physician before it is transferred to the medical record department, in which case it is usually sent to the "Doctors'



Room" or left out near the medical record department to be completed by the attending physician. These areas are often left unlocked. Our investigation revealed variations in the time for completion of the record and filing with the medical record office from 48 hours to one month after the patient's discharge.

Copies of the final summary are made and sent to the various staff members involved in the patient's treatment, including the attending physician, surgeon and any other consultant. At the time of our hearings, The Wellesley Hospital retained the physician's copy of the final summary in the medical record department for those who wanted them. Physicians did not often want them with the result that at the end of the year hundreds were left. There was no written policy relating to the disposal of these but, in practice, they were torn up and disposed of.

When completed, the medical records are filed away, usually using a colour coded numbering system with a central alphabetical index file. This means that to locate the medical record it is first necessary to look up the patient's central index card (filed alphabetically by patient name) to find and interpret the necessary location code for the medical record, a procedure which prevents the records from being easily accessible to unauthorized personnel. While this card augments the security of the medical record, it, in turn, itself becomes a handy source document for such potentially sensitive information as the patient's address, date of birth, attending physician, next of kin, admission and discharge dates, and OHIP number, information which was sometimes disclosed to third parties. In hospitals like the Manitoulin Red Cross Hospital in Mindemoya, and the Hotel Dieu of St. Joseph's Hospital in Windsor, this separate index card also contains the patient's diagnosis.

Although nurses' notes are commonly included and stored as part of the medical record, it seems to be just as common for these notes to be separated and stored independently by being filed according to the patient's discharge date and alphabetically by his or her name. This makes them easier to locate than the medical record. Emergency sheets and out-patient records are also maintained separately in a number of hospitals' medical record departments, as are such documents as patients' certificates for abortion.

The medical record department is by far the most secure area in most hospitals. In order to determine how securely most hospitals maintain their medical records, as part of our investigation, members of the Ontario Provincial Police surveyed 265 Ontario public, private and psychiatric hospitals between January and February 1978. The quality of security varied

considerably from hospital to hospital, but on the whole it was poor; this is how the investigator in charge of the survey, Detective Sergeant R.D. Fulton, summarized the findings:

It is obvious that security in the majority of hospitals is inadequate. It is believed that the administration and staff do not realize the proper meaning of security. This may be an area where our Security Branch could make surveys and recommendations.

The medical record storage area in most hospitals is locked only when left unstaffed. It is unusual for the files themselves to be locked and only a few hospitals, such as the Northwestern General Hospital in Metropolitan Toronto, lock the identifying alphabetical index cards when the department closes. In most hospitals the keys to the medical record department are held by a limited number of hospital administrators, directors, supervisors and senior personnel so that access to the department by other personnel must come through these key-holders in off hours. Sometimes the key is kept in a central location, such as the switchboard or admitting department for use by appropriate personnel.

The staff of a medical record department usually includes an accredited medical record administrator or librarian and technician, who are professional persons specially trained to handle confidential patient information. Most of the department's members, however, are clerks, secretaries and transcription typists, with no special medical record background or education. All of the department personnel have access to the medical records. The numbers vary with the size of the hospital. The Toronto General Hospital's department has more than 100 employees.

By virtue of section 42 of Regulation 729, medical records that have been photographed must be retained for two years from the date of discharge or death of the patient. The photographs (in practice, microfilm) must be retained for 50 years. Section 44 requires that if they are not photographed the original medical records must be kept for 20 years (unless the patient has died, in which case the period is five years). As a result of these requirements the medical record department is in charge of an extraordinary number of patient records whose storage, release, access, security, retention and destruction it must control. In order to discover what policies and procedures hospitals in Ontario had developed to regulate the protection of patient information we wrote to 232 public hospitals, 12 psychiatric hospitals and 375 nursing homes and asked for a copy of

the "by-laws, executive or administrative decisions, or other internal regulations" governing the confidentiality of health-related information in their establishments. We received replies from 158 hospitals and 115 nursing homes, answers which generally gave quite a discouraging picture of confidentiality-protection procedures in Ontario health-care centres. Of those replying, a few hospitals and most nursing homes said that they had no written policies and were guided solely by the provisions of The Public Hospitals Act, The Mental Health Act, or The Nursing Homes Act, 1972, as the case may be. Some hospitals admitted that our inquiry had stimulated them to draft the guidelines which they sent. Still others sent copies of policies taken from medical record-keeping textbooks or American papers on the subject. One hospital claimed to follow the Guide to Hospital Accreditation, yet this guide advises the hospital to "develop and adopt" its own "by-laws, rules and regulations", something which this hospital apparently had not done.

The policies of some hospitals were inadequate and there was little consistency between the policies of the various hospitals, not surprisingly, in light of current inconsistent legislation with respect to confidentiality. For instance, policies as to the amount of patient information which is released to the police varied considerably from hospital to hospital. Most hospitals' guidelines covered only the medical record department; other departments were not even governed by hospital guidelines.

However, some policies were excellent. Hospitals in a few Ontario districts had met to propose model policies for the facilities in their area. The Hamilton region's proposals were the most comprehensive and widely adopted, and were included, as a model, by the Canadian Health Record Association in its brief prepared for the purposes of our inquiry.

### The Accounting Department

The information on the original OHIP 106A form, including the patient's physicians' names and provisional diagnosis, is transposed onto an account ledger card and maintained in the accounting department. Prior to a change in the OHIP hospital claims system in 1979 to utilize the services of the Hospital Medical Records Institute (HMRI), it was usual for the accounting department also to receive discharge information about every patient released from hospital, in order to prepare cards to be sent to OHIP. The standard OHIP form 106D (the "D" indicating a discharge form) required the discharge diagnosis and information about any operations or therapeutic procedures performed for the

patient during the hospital stay. This discharge information usually came to the accounting department from the floor or from the medical record department in the form of a final discharge summary, but we discovered that, in some cases, the patients' accounts department received much more than a discharge summary. For example, at North York General Hospital, clerks handling out-patient accounts received a copy of the full patient's chart to obtain accounting information relating to out-patients. It seems unlikely that the clerical staff in the accounting department needed access to all of this medical information in order to be able to extract a limited amount of diagnostic and procedural information. Under the new billing system, the tasks of reviewing the medical records, determining the patient's diagnosis and procedures, and completing the HMRI abstracts are all performed in the medical record department by persons whose job it is to complete medical records, thereby limiting the amount of information seen by the accounting clerks.

Accounting departments retain patients' account cards in case any patient calls to have his or her account clarified. In their reports to their customers, private investigators often indicated that they had obtained such information as the patients' dates of hospitalization or treatment, hospital and family physicians' names, and the patients' OHIP numbers from the accounting departments of hospitals in Ontario. With respect to physical security, the recent information kept by the accounting department is usually kept in open drawers and unlocked cabinets.

## Confidential Information

Although legislation is not, by itself, a complete answer to all threats to the privacy of patient information maintained by health-care facilities, if it can clearly define both the responsibilities of the health-care facility in safeguarding confidentiality and the rights of its patients to the maintenance of protection, it will provide what the U.S. Privacy Protection Study Commission spoke of as a "legitimate, enforceable expectation of confidentiality." The first determination that must be made is the scope of information that should be protected by the new legislative measures. What information maintained by hospitals and other health-care facilities should be treated as confidential?

Earlier I pointed out that patient information that is not attached to a hospital's medical record receives much less attention and protection as far as confidentiality is concerned than does the medical record itself. This practice arises out



of the legislation, for although the administrator of a public hospital "is responsible for the safekeeping of all records relating to a patient", it is the limited "medical record" or "information from a medical record", the disclosure, retention, microfilming and destruction of which are the subject of the information protection provisions of Regulation 729. In subsections 1-8 of section 26a of The Mental Health Act, access to and disclosure of "the clinical record" is what is regulated, (although subsection 9 has a broader scope and will be discussed subsequently).

Because legislation defines the medical or clinical record as the document to be protected, and most hospital personnel consider this record to be the most complete and useful source of medical information, other patient-identifiable health-related information receives few, if any, safeguards. As a result, many primary reports relating to patients' care and treatment, such as emergency department sheets, nurses' notes, blood bank requisitions, and social service records, which are not attached to the medical or clinical records, are maintained in various hospital departments by staff who are untrained in record-keeping and who may be without the benefit of an ethical code to follow.

Secondary records, such as index cards and accounting forms containing health-related information extracted directly from the medical record are often treated as something less than confidential. If the information in a medical record is extracted and put into another document to be used for a different purpose, the information in that other document does not receive the same care that is required for the medical record itself under the existing legislation.

Similarly, there is a good deal of evidence that when primary reports which are a part of the medical record are mimeographed or carbon-copied, the copies, in many quarters, are not considered part of the medical record, even though they contain exactly the same information as the original document. An example is that of laboratory report copies which section 35a of Regulation 729 directs be retained in the laboratory, while the original is to be made a part of the medical record. At our policy hearings Roger Slute and Judith Moran of the Ontario Hospital Association had the following discussion with Mr. Sharpe, acting as Commission counsel:

MR. SHARPE: But the OHA hasn't considered whether or not copies two, three, four and five of pathology reports would be



considered to be part of the medical record, as well as the original?

MR. SLUTE: No. We have assumed they are not part of the medical records. They are kept for some other purpose. The medical record is that file folder for all its future patient use, benefit and for all the legal possibilities, whatever, the medical record. Now how many copies there are floating around, no. We have not...

MISS MORAN: I could just comment that as far as the medical record is concerned, the original that is made is the medical record, the part for the medical record. Other copies then are agreed upon for other areas of the hospital or doctors, but I don't think as far as the medical record department is concerned then that is part of the medical record. As far as they are controlling for legal, you know, release of information, things like that.

It may be reasonable, from an administrative point of view, for hospitals to think of copies of such documents as pathology reports as distinct and separate from the official medical record. However, from the point of view of the protection of the confidentiality of the patients' sensitive information contained in these copies, this assumption may lead to the result that measures required by law to protect confidentiality are felt to have no application. This interpretation came to light when copies of pathology reports from The Wellesley Hospital were spilled in downtown Toronto, and the Minister of Health informed the Legislature that no breach of The Public Hospitals Act or its regulations had occurred because the pathology reports were merely duplicates. Hansard for June 23, 1978, records this statement by the Honourable Dennis Timbrell:

The distinction between copies of records and the actual records themselves is an important one, because the current regulations under the Public Hospitals Act do not cover disposable materials of this kind; that is, duplicate or extra copies of records. The regulations deal only with what be termed the formal medical records of the hospital or photographic copies made for a permanent record.

...In this case I am advised that there has been no contravention of the Public Hospitals Act or its regulations, but obviously the Wellesley case shows there is a loophole in the regulations.

Although as a matter of statutory interpretation it may be said that copies of documents do not form part of the medical record, it is not right that, by virtue of that fact, they should be deprived of the protection to which the original copies, which are part of the medical record, are entitled. The "loophole" to which Mr. Timbrell referred should be closed.

The testimony at our hearings revealed that such information as the patient's admission and discharge dates, OHIP number, address, next of kin and attending physician was commonly considered by hospitals to be non-medical in nature and, as a result, was frequently released to outside inquirers. Information of this sort is health-related and may therefore be sensitive. Both the fact of admission and the nature of the facility, for example, a psychiatric hospital or a cancer treatment centre, can provide information about the health and treatment of a patient which must be considered confidential.

The Patients' Rights Association proposed an expansion of legislative protection to include all oral as well as written health-related information:

Legislation should protect the confidentiality of health information generally, and not just of health records. It is unacceptable that third parties should be allowed to obtain health information through oral communications or through written communications which do not form part of the health record, in situations in which they are not permitted access to the health record itself.

In my view, the Association's point is well taken.

What is necessary is the fullest possible protection of the hospital patient's privacy, and it is obvious that the present legislation fails to offer this. Statutory protection must be given to the confidentiality, not only of the medical records, as defined by legislation or regulation, but of all the primary reports, notes, materials and secondary records, whether originals or copies, written or oral. One way of accomplishing this objective is illustrated by the provisions of section 26a(9) of

The Mental Health Act, which, subject to the consent of the patient or the interests of justice, prohibits disclosure in an action or proceeding in any court or before any body, not merely of the "clinical record" but of "any knowledge or information in respect of a patient obtained in the course of assessing or treating or assisting in assessing or treating the patient in a psychiatric facility or in the course of...employment in the psychiatric facility...". Protection of patient information in hospitals can be strengthened by adopting a similar formula. The recommendation that follows should be read subject to what is said later about authorized disclosure of a patient's health information.

#### *Recommendation:*

46. *That legislation protecting patient information in hospitals and health-care facilities be made applicable to any knowledge or information pertaining to the health, care, assessment, examination or treatment of the patient, unless the knowledge or information is in a non-identifiable form.*

The broad scope of this recommendation is intentional. Our evidence and research make it clear that there is no hospital information that some patients do not consider to be confidential, including the names of their physicians, the dates of their hospital admissions or discharges or even the very fact of their hospitalization. The words "any knowledge of or information" are intended to include information which is not documented or recorded in any form, and which an employee possesses.

## Record Management

An important factor in many of the incidents investigated involving violations of the confidentiality of hospital patient information was the hospitals' inadequate policies and procedures for information management. Information management includes the methods by which these facilities routinely deal with the collection, retention, security, destruction and dissemination of their confidential patient information. Controlling the handling of this information poses a unique and complex administrative problem for every health-care institution because of the variations in size, personnel, services and available facilities. Improving the present practices of hospital information

administration is central to any enhancement of the protection of their patients' health-related information.

The role of legislation in the creation of adequate practices of hospital information management is not to attempt to dictate detailed administrative procedure to hundreds of divergent health-care facilities. Its function is to bring into existence standards and responsibilities, requiring individual health-care institutions to meet these standards in the manner their particular capacities allow. In other words, the legislation should not attempt to dictate such matters as how all hospitals should store their patients' files or by what means they should destroy them; instead it should enact the criteria to be satisfied with respect to the storage and destruction of confidential patient information. It is worth noting that the enactment of legislative standards of record management for health-care providers was proposed as a "model option" in the Final Report to the Ford Foundation of the National Commission on Confidentiality of Health Records in the U.S.A. In the following pages general responsibilities and principles for controlling the collection, retention, security, destruction and dissemination of the confidential information within hospitals and health-care facilities are suggested.

The effective implementation of legislative standards of information administration requires that health-care centres develop their own individual policies and practical procedures in accordance with the standards. During the course of our inquiry the importance of every institution having written rules and regulations to regulate the confidentiality of its patient information became increasingly clear. For instance, one of the prime factors behind the accidental dispersal of hospital pathology reports in patient-identifiable form in downtown Toronto was the hospital's lack of any written policies with respect to the proper method of destruction of these documents for reference by the hospital's staff. This is by no means surprising as our survey revealed that, in general, the written policies and procedures in Ontario's hospitals are inadequate. I endorse the Canadian Health Record Association's emphasis, in its brief, on the importance of individually developed record-management policies.

*Recommendation:*

47. *That legislation governing the confidential information maintained by hospitals and health-care facilities require each hospital or health-care facility to develop its own policies and*

*procedures, compatible with the legislation, to regulate the collection, retention, storage, security, access, release and destruction of all confidential patient information.*

Although the creation of a standardized set of administrative procedures for all of the hospitals and health-care centres throughout Ontario has been suggested as a means of promoting confidentiality, the differences in the services and methods of operation of these facilities make complete uniformity impractical. Many of the hospitals surveyed asked for flexibility in meeting their own individual circumstances and particular problems. At the same time many requests were made by hospitals for guidance in applying the legislation. Although I make no formal recommendation in this regard, I believe that it is desirable that the Ontario Hospital Association, in collaboration with other appropriate associations and Ministries with legislative responsibility for the institutions and facilities affected, develop a set of practical prototype policies and procedures for information management for the assistance of hospitals and health-care facilities in the development of their own procedures.

An important prerequisite for the effective application of statutory standards of information control is the designation or appointment by every hospital of an information manager. Although under section 39(2) of Regulation 729 under The Public Hospitals Act the "superintendent is responsible for the safe-keeping of all records relating to a patient", we found little evidence that hospital administrators create a centralized, coherent system of information management for all of their confidential patient information. Our research and investigation revealed that the procedures in most hospitals varied from department to department, as did the quality of the protection of the confidentiality of material in the departments. For example, if a private investigator was unable to obtain any information about the claimant he was investigating from the medical record department of a particular hospital, he made inquiries at other departments of the same hospital and, in most cases, received the information which he had originally been refused. Many hospitals have no official administrative procedures to control information in any department other than the medical record department. The individual designated as information manager should have clearly defined responsibilities for co-ordinating internal hospital policies and procedures for information management.



Many hospitals and health-care facilities in Ontario do employ a professionally trained health record administrator, formerly known as a medical record librarian, or a health record technician to manage the records in the medical record department. In October, 1978, in an address to the Canadian Health Record Association, the Minister of Health, Mr. Timbrell, encouraged the members of the Association to expand their area of responsibility to include the management of all records within their hospitals that contain confidential information. During our policy hearings I asked Janet Milner, executive director of the Canadian Health Record Association, about the feasibility of giving the health record administrator control over the care and custody of all records wherever they may be found in the hospital and not only in the medical record department:

MR. COMMISSIONER: Is there a practice anywhere in Canada in which in fact it is understood that the person who has the jurisdiction and the responsibility for seeing to the content and the care of those records is the person in charge of the medical records department?

MRS. MILNER: I could speak to that. At the Health Sciences Centre in Winnipeg that's the case. One of our senior people that would take charge there, she has complete jurisdiction of all medical communications within the complex, including radiology, lab. She has people that she dispatches to these areas of the hospital, to the different services in the hospital, and they are in charge of seeing everything is done correctly at the source of protecting privacy.

She has a different type of title though, and looking at the title I wouldn't want to make a definitive statement on what her relationship is within the structure, the administrative structure of the hospital, but it certainly is not a line situation with the head of x-ray or the lab or so on. It's a little bit different.

MR. COMMISSIONER: What about the communications that are made to the outside world by whoever answers the telephone when an inquiry is made about a patient? Would she be responsible for that as well?

MRS. MILNER: Yes. And policies that are written into the department or the hospital manual so that people within all of these jurisdictions are required to adhere to, not just the people who have formal training in health records.

The Canadian Health Record Association considers it realistic for an information manager trained in health record science to co-ordinate privacy protection for an entire institution, and the Ontario Health Record Association agrees:

We believe that the health record administrator/technician in charge of the medical record department in a facility, should, as delegated by the administrator, have complete control of all patient documentation, whether centralized or decentralized. We believe that this department head should be responsible for the formulation of policies for the control of copies of records as well as originals and their safe destruction at the appropriate times. We further believe that this department head should be responsible for the adherence to these policies by any department within the hospital having within their area either original or photocopied records or information therefrom.

The Ontario Health Record Association does not expect the advent of the computerization of hospital medical records to affect its members' information management function. The Association takes responsibility for ensuring that their members will be able to deal with the computerized clinical record and are supporting research being done at the University of Western Ontario with respect to a post-graduate course on health record administration in computer science.

Given the size and needs of some of our hospitals and other health-care facilities, it would not be realistic to require that all of them employ a qualified health record administrator. Some of them, indeed, would find his or her qualifications disproportionate to their modest capacity. What is not unreasonable, however, is that every hospital administrator be required to appoint an information manager.

*Recommendation:*

48. *That legislation require the administrator of every hospital to appoint or designate an information manager, to be responsible for implementing and co-ordinating the policies and procedures for management of all patient information in the hospital. In the absence of such an appointment, the responsibilities and duties of information manager should reside in the administrator.*

Although only the information manager requires formal training in protecting confidentiality, all persons working in the institution must be instructed about the importance of, and need for, maintaining patient privacy and trained in their practical duties and responsibilities in safeguarding patient information. Our investigation of various incidents in which confidential information was inappropriately disseminated by hospitals disclosed a basic lack of awareness and understanding on the part of many hospital employees of their responsibilities as defenders of confidentiality. Although an increased sensitivity to the significance of confidentiality resulted from the publicity given to our inquiry, there is a demonstrated need for an effective educational programme for hospital employees to ensure their awareness of the requirements of confidentiality.

Hospitals often ask applicants for employment, on their personnel application forms, to agree to maintain confidentiality if they are hired, and then touch upon the subject again during the new employee's general orientation to the hospital. These practices are commendable but fall short of adequately educating the employee about his or her responsibilities for the protection of the privacy of identifiable patient data. What is needed is a comprehensive programme of employee education. The Canadian Health Record Association made this submission in its brief:

All persons having access to the health information as part of their employment or specialized training, should be specifically informed of their individual responsibility to protect the confidentiality of all health data, and of any consequence of violation of the policy. It is strongly recommended that there be a penalty attached for this by the employer and written into personnel policies.

It is preferred that a "Pledge of Confidentiality" be used to ensure employee awareness of the responsibility. However, where this may not be possible, a "Statement of Understanding" should be signed on employment and renewed annually.

Where persons having access to the data are subject to a "Code of Ethics" or a professional oath which includes a requirement to protect health information, the signing of a Pledge or Statement may be waived.

It is reasonable that hospitals should be required to inform their employees "of their individual responsibility to protect the confidentiality of all health data", and to introduce them to and instruct them in those written policies as they apply to their tasks. It is equally reasonable that employees should be informed of the possible sanctions for violation of their responsibilities.

The penalty for contravening The Public Hospitals Act or its regulations is set out in section 36 of the Act in the following language:

Every person who contravenes or is a party to the contravention, directly or indirectly, of any provision of this Act or the regulations is guilty of an offence and on summary conviction is liable to a fine of not less than \$25 and not more than \$500.

During our hearings investigating the RCMP's alleged access to confidential patient information it was argued that section 36 does not affect hospital employees. Section 48(1) of Regulation 729 imposes on the board of a public hospital the duty not to permit any person to receive information from a medical record. I have already recommended that information deserving protection should not be limited to the medical record. With respect to confining the duty to the board, as opposed to all employees and other persons working in a hospital, Mr. Justice Dubin addressed this issue in the judgment of the majority in the Court of Appeal in Re Inquiry into the Confidentiality of Health Records in Ontario (1979), 24 O.R. (2d) 545 at page 561:

Section 48(1) in terms specifically relates only to the board of a hospital and not to all hospital employees or other persons under the direct control of the board, and

the penal provision of the statute appears only to be directed to the board or those persons who are parties to any breach by the board. However, it is implicit, in my opinion, having regard to what is stated in the regulation when read as a whole, that hospital employees or others under the direction of a board are under a like duty not to permit any person to remove, inspect or receive information from a medical record other than in a manner which is authorized in the regulation or under any other due process of law.

What is implicit in the scheme of the legislation should be expressed in clear and unambiguous language.

After an employee has been properly informed of the institution's policies on confidentiality and of the sanctions for breaches, and required to acknowledge his or her understanding of this information in an appropriate manner, the education of the employee should not end. Policy manuals containing the rules and procedures for protecting patient confidentiality should be made readily available throughout the hospital for reference purposes and instruction as to changes or updating of procedures provided when necessary.

*Recommendations:*

*49. That hospitals and health-care facilities*

- (a) inform all employees of their individual responsibility to protect the confidentiality of patient information;*
- (b) instruct all employees in the institution's written confidentiality policies; and*
- (c) inform all employees of the penalties for the violation of these policies.*

*50. That legislation governing hospitals and health-care facilities impose on all employees and other persons working therein, the duty not to release*



*patient information without the consent of the patient except when required or permitted by law.*

From the structure of information management, I now turn to the actual handling of confidential information, that is, its collection, retention, storage, dissemination and destruction.

The primary purpose for which hospitals and other care facilities collect confidential information about their patients is to provide proper health care. The information collected for this purpose is extensive, often including a patient's full social and family history, as well as details of his or her personal and emotional experiences. The physician may also include observations about the family and friends of the patient, and note subjective comments about the patient made by these persons. The nature and quantity of information collected for the purpose of patient care depend upon the patient, the physician and the type of treatment required.

During the 1978 address to the Canadian Health Record Association to which I referred earlier, Mr. Timbrell expressed an important goal of information management:

Without interfering with medical practice,  
we must restrict the amount of information  
on file...

Any attempt on my part to make recommendations which might limit the amount or type of information which may be collected for health-care purposes would rightly be perceived to be an interference with the practice of medicine or the provision of health care. I shall therefore refrain from doing so. It seems to me, however, that the right of access by patients to their records will encourage the recording of only that information that is essential for proper patient care.

Institutions sometimes collect confidential information about their patients for secondary purposes, such as for use in research projects or education. Although it may be legitimate to use confidential information for such purposes under certain circumstances, I agree with the position of the American Medical Record Association that "the types and amount of information gathered and recorded about a patient shall be limited to that information needed for patient care." The collection of information extrinsic to the patient's assessment or treatment because of its relevance to a clinical research project or an educational programme underway at the hospital is an invasion of

his or her privacy, if it occurs without his or her knowledge and consent.

*Recommendation:*

51. *That legislation provide that a hospital or health-care facility may collect only information required for the care, assessment, examination or treatment of the patient unless he or she consents to the collection of information for other purposes.*

Health-care facilities should also endeavour to ensure that the patient information which they collect and retain on file is both accurate and complete, since failure to do so can have serious consequences for the patient. Again, the right of patient access and a procedure for correcting errors should encourage the adoption of reasonable procedures for ensuring accuracy.

One way of restricting the amount of information on file is to limit the period of time for which it must be retained. At present the information in public hospitals is governed by a variety of retention provisions found in Regulation 729. The storage schedule for the medical record in a public hospital is set out in sections 42, 44 and 45 of Regulation 729 (as amended by O. Reg. 100/74, section 8):

42. (1) Where medical records are photographed in order to keep a permanent record thereof, such photographing shall be carried out in accordance with a practice established by the board after considering a recommendation from the medical advisory committee, for the photographing of medical records of patients and out-patients.

(2) Medical records that have been photographed pursuant to subsection 1 shall be retained for two years from the date of discharge or death of the patient and may be destroyed thereafter by the administrator.

(3) Photographs made pursuant to subsection 1 shall be retained for fifty years from the date when they were made and may be destroyed thereafter by the administrator.

. . . . .

44. Medical records that have not been photographed in accordance with a practice established by the board pursuant to section 42 shall be retained by the hospital,

(a) for twenty years following the date of the discharge of the patient or the date of the last visit of the out-patient, as shown on the medical records; or

(b) for five years following the death of the patient or out-patient,

and may be destroyed thereafter by the administrator.

45. (1) The medical record of a patient or of an out-patient under eighteen years of age may be photographed and destroyed in accordance with the provisions of sections 42 and 43.

(2) Where the medical record of a patient or of an out-patient under eighteen years of age is not photographed pursuant to subsection 1, it shall be retained,

(a) for twenty years after the eighteenth anniversary of the birth of the patient or the out-patient, as the case may be; or

(b) where the patient or the out-patient is deceased, for five years after the patient or the out-patient, as the case may be, would have become eighteen years of age if he had lived.

The quantity of information maintained by Ontario hospitals by virtue of these retention requirements is difficult to imagine, and the provision of secure storage becomes an onerous burden. The retention schedule is intended to serve future needs for the record for patient treatment, in court actions, and for other functions such as research, teaching and statistical analysis. These needs are valid, but under the existing scheme highly sensitive documents are being kept longer than is reasonably necessary to meet these needs, increasing the risk

that their confidentiality will be breached, a risk that must be considered in determining acceptable retention periods.

It is not unreasonable to ask how frequently old medical records of discharged or deceased hospital patients are actually used for any purpose. The Report of 1978 of the Ontario Council of Health on Medical Record Keeping provides the following information at page 17:

A survey on the retrieval pattern of old charts was carried out in a number of hospitals, including a major teaching hospital and a large community general hospital. A fairly consistent pattern of reference to old charts emerged from the study, i.e., that after three years, the number of requests for retrieval becomes insignificant. While the results of the survey may not be applicable to all hospitals in Ontario, it is felt that a change in legislation, reducing the mandatory retention period would benefit the majority of hospitals, with consequent economies. However, such legislation should be of a permissive nature, giving hospitals with particular needs the option of continuing with their current policies.

The evidence suggests that only a minimum of information from a patient's record--information such as the patient's full identifying data and record summary--need be retained for a lengthy period of time.

Regulation 729 includes retention schedules for documents and materials apart from the medical record which have also been questioned. Reference has already been made to section 35a(2) of Regulation 729, which requires that copies of all laboratory reports remain in the laboratory for a three-year period. The Ontario Hospital Association criticized this requirement of retention in an area of the hospital not geared to record maintenance as an example of "bad law", dangerous to confidentiality. In ordinary circumstances, "Nurses' notes, charts showing temperature, blood pressure and respiration, sheets showing vital signs or fluid balance and other notes not made by a physician", are not part of the medical record and have their own retention period which is found in section 46 of Regulation 729. Materials such as x-ray films and tissue slides made for microscopic examination also have individually designated retention periods under Regulation 729 (as amended by

O. Reg. 100/74, section 9) in sections 47 and 47a respectively. In its brief the Ontario Hospital Association expressed the view that "it is neither necessary nor desirable to establish mandatory periods in law for retaining such materials where a written interpretation, or result, of a test or examination is placed in the medical record."

Although the presence in the legislation of various locations and retention periods for different types of patient-identifiable records and materials held by a hospital increases the difficulty of maintaining the confidentiality of this information, a minimum storage period is necessary for medical and such other reasons as the two-year limitation period for commencing action against a public hospital or hospital employee. However, the existing legislation dictates extensive retention periods for large amounts of patient information without taking into account duplication and actual utility, at a risk to patient privacy. I propose that the present retention schedules for medical records and all other sensitive documents and materials be examined, and, where necessary, the legislation be amended to ensure that confidential patient information is not required to be retained in a form or location that is inappropriate, or for a period that is longer than is essential.

*Recommendation:*

52. *That the legislation and regulations requiring hospitals and health-care facilities to retain patient-identifiable health-related documents and materials be reviewed and, where necessary, amended, to ensure that patient information is retained in an appropriate manner and for a period which is consistent with minimum medical and legal requirements.*

Hospitals, we have seen, maintain patient-identifiable, health-related information in their medical record departments, in many other departments, on the ward (temporarily), and in designated storage areas such as separate rooms, basements, and perhaps storage sites off the hospital premises. Confidential patient information may be stored in paper form or on microfilm, microfiche, or even in a computer. The computerization of hospital medical records now exists on a very small scale in the Province, but experts predict a marked increase in hospital use of computers in the next five to ten years. At the present time, most hospitals retain their confidential patient information in hard copy or paper form, and microfilm the inactive



medical record after a period of time for convenient long term storage.

All of the confidential information maintained by a hospital must be kept physically secure if the patient's privacy is to be protected. Although the administrator of a public hospital "is responsible for the safekeeping of all records relating to a patient", our investigators discovered that the confidential information in these institutions is, in general, far from secure. The widespread practice of keeping sensitive health-related information in open drawers and shelves, unlocked filing cabinets, unsupervised offices and publically accessible areas is far from satisfactory. Keeping this information both accessible for authorized use and safe from improper access poses a security challenge unique to each hospital. The information manager of each institution must work out the particular policies and procedures for maintaining an adequate standard of physical security for all the confidential information under his or her jurisdiction. I have recommended that policies and procedures be created to regulate retention, storage and security of patient information, and these policies and procedures must provide for an adequate standard of physical security.

*Recommendation:*

- 53. That all hospitals and health-care facilities maintain their confidential patient information in designated areas which are physically secure, under the immediate control of designated persons and not accessible to or available for inspection by unauthorized persons.*

A rule that confidential information be retained no longer than is necessary implies the prompt destruction of all obsolete patient-identifiable materials. Information managers must arrange for the establishment of written retention schedules for all confidential documents and materials within their institutions (not inconsistent with the terms of the legislation), according to which these documents and materials must be destroyed by designated personnel. Moreover, the destruction of this information must be carried out in such a manner as to ensure that the patients' confidentiality is safeguarded throughout. For example, during our hearings in London, it was suggested that we investigate the manner in which patient records of Victoria Hospital were being kept while awaiting destruction. Our investigators found that, prior to their destruction in the hospital shredder, these documents were left unsecured and easily accessible to unauthorized persons. To its

credit, as soon as it learned of the situation and within hours of our investigators' visit, the hospital purchased a lockable steel cage to hold the records securely while awaiting destruction. Safeguarding the confidential material which it is preparing to destroy must be a recognized part of every facility's destruction procedure.

On another occasion various types of patient-identifiable hospital documents from the Salvation Army Grace Hospital in Windsor fell from a contractor's truck and were dispersed at a city intersection. However, it was our earlier investigation of the spillage of a large number of pathology reports belonging to The Wellesley Hospital from a disposal truck onto downtown streets which revealed another aspect of the destruction process to which attention must be paid--the hospital's failure to specify either orally or in writing the method of destruction for these reports. The clerks responsible for disposing of the pathology reports testified that, while their impression of the proper mode of destroying these reports was to tear them in half and deposit them in waste containers, they had not torn them at all because they were short of time that day. Mrs. Ellen Barnes, director of medical records of The Wellesley Hospital, testified that there were no specified methods of destruction for other confidential documents, such as discharge summaries and nurses' notes, a deficiency which she said was not uncommon in hospitals:

Q. Without naming any other hospital, have you had, have you worked in the medical records section of any other hospital?

A. Yes, I have.

Q. How many hospitals?

A. Four that I can think of off hand.

Q. Did any of those hospitals have memoranda which set out the manner in which documents such as discharge summaries, the yellow copy of form eighty-five and nurses' notes would be destroyed?

A. No. The nurses' notes though come under, because they are bulk and they are not done that often, that is a large disposal and dealt with as it comes up in the best manner....But in any other department I have worked in, there have been no

directives to me or from me as to how to destroy day-to-day records in a department.

In the case of the official medical record, most hospitals do have a designated method of destruction, and so should there be for every type of confidential document or article. The method of destruction selected will depend upon the type of document concerned and the facilities of the institution. Many hospitals now destroy their records through shredding or incineration. Erasure of computerized information will probably occur more frequently with the increasing computerization of records. The destruction process must render all confidential information completely and permanently non-identifiable, and any method which can accomplish this is acceptable. As The Wellesley Hospital's experience shows, failing to tear copies of records in pieces and sending them to an outside disposal site on the back of an open truck, is not an adequate means of destruction.

The Wellesley Hospital incident points up the need for a control system to ensure that destruction does occur in the specified manner. The destruction of confidential information should occur under the supervision of responsible personnel designated by the information manager, personnel who can also act as witnesses to the fact that the information was indeed destroyed. Section 43 of Regulation 729 requires that when the medical records in a public hospital are destroyed, the particulars of the destruction and the information involved must be set out in a statutory declaration:

When medical records or photographs thereof are destroyed, the administrator shall forthwith make a statutory declaration under oath stating the date and manner of the destruction, the fact that the destruction was carried out in accordance with a practice established by the board pursuant to section 42 and the names of the patients whose records or photographs of records were destroyed, and the administrator is responsible for the safekeeping of such declaration.

While there is merit in requiring a statutory declaration to certify the destruction of the medical record, it may not be necessary to so document the destruction of the many other types of confidential information. However, a log briefly recording the general categories of confidential information destroyed

should be kept in all cases. The following standards should form part of the policies and procedures recommended previously.

*Recommendation:*

*54. That hospitals and health-care facilities*

- (a) provide for destruction procedures for all types of patient information which will render the information completely and permanently unidentifiable;*
- (b) safeguard the confidentiality of the information during the entire destruction process, including the period it is awaiting destruction and while being transported to the site of destruction;*
- (c) destroy confidential information according to a written retention schedule consistent with the terms of legislation; and*
- (d) record the particulars of the destruction in a log or by statutory declaration where required by law.*

A small but growing number of hospitals send their medical records to service organizations for microfilming, relying on these organizations to destroy their records after microfilming them. The hospitals cannot exercise control over the destruction process in these circumstances. In a survey conducted by the Ontario Hospital Association on methods of destruction of medical records in member hospitals, one hospital administrator had the following to say about this practice:

We are concerned with this (microfilming companies destroying medical records) because frankly people are employed by these companies who in my opinion from time to time don't really care what happens to the records although I believe the officials of the companies are keen and really try to do a good job. At one time we did receive a certificate stating that certain records had been destroyed and they were later returned

to us. Needless to say, we are not dealing with that company at the present time.

This problem will be dealt with later.

## Access and Disclosure

The information manager should have responsibility for monitoring both the access to and the disclosure of all the confidential patient information under the jurisdiction of the health-care institution. Because of the growing use of health information by persons other than those directly involved in providing health services, the task of regulating information dissemination is an enormously complex one. Hospitals and other care-providing establishments regularly receive requests for patient information from employers, insurance companies, government agencies, inspectors, lawyers, schools, family members, social agencies, police officers, coroners, members of the press, other health-care providers, professional colleges, researchers, teachers, their own employees, the patients themselves and many others. The number and type of requests received depend on the size of the hospital and the type of service it provides, with some large general hospitals reporting hundreds, sometimes thousands, of requests each month.

The release, inspection or removal of information from a patient's record is prohibited under both Regulation 729 under The Public Hospitals Act and section 26a of The Mental Health Act, with exceptions under certain circumstances and to designated recipients, and those who have the consent of the patient. Valid interests that conflict with the patient's right to privacy sometimes transcend patient confidentiality, and it is appropriate, therefore, for the legislation to continue to authorize disclosure in those cases in which other interests outweigh the patient's right to privacy, while prohibiting all other disclosure unless the patient consents. Although such legislation does not give the individual complete control over access to his or her confidential health information, it puts limits on non-consensual disclosure and provides patients with what the U.S. Privacy Protection Study Commission called the "basis for an expectation of confidentiality." However, the present Ontario legislation governing the disclosure of patient information from health-care institutions lacks uniformity and consistency. As I have already pointed out, the authorized recipients of "information from a medical record" in a public hospital are designated along with the circumstances of the disclosure permitted, whereas another group of persons under a



different set of circumstances is permitted access to the clinical record of the patient of a psychiatric facility.

Legislation governing the situations in which the patient's confidential information is permitted to be disclosed should be very specific in nature. As the U.S. Privacy Protection Study Commission said in its report, Personal Privacy in an Information Society, at page 305, "the individual cannot rely on his expectation of confidentiality in any record-keeping relationship unless the restraints on disclosure are known." The present legislation affecting hospitals and psychiatric facilities fails to impose limitations on the disclosure of their patients' confidential information. For example, under section 48(5)(b) of Regulation 729 an administrator of a public hospital may be permitted "to inspect and receive" confidential information from a medical record in another hospital after making a written request for the information, without indicating the purpose for which disclosure is requested. Permitting an individual or organization to receive confidential information otherwise than for specified purposes, is difficult to defend. On the other hand, authorizing access for a particular purpose without identifying the persons permitted to use the information for this purpose is also unjustifiable. Section 26a(3)(f) of The Mental Health Act provides that:

...the officer in charge may disclose or transmit the clinical record to or permit the examination of the clinical record by,

. . . . .

(f) a person for the purpose of research, academic pursuits or the compilation of statistical data.

Of course, it is not possible to pinpoint the precise identity of every type of user, but it is not satisfactory for the legislation to fail to identify a class of users or to require an authority for the particular recipient's access.

The present legislation governing access to patient records in hospitals or psychiatric facilities is also inconsistent with provisions for access under other provincial legislation. For example, under section 52 of The Workmen's Compensation Act, R.S.O. 1970, chapter 505 as amended by S.O. 1973, chapter 173, section 1, "every hospital official...shall furnish to the Board from time to time...such reports as may be required by the Board in respect of such employee." There is, however, no complementary authority for a hospital to release patient information to

the Board in The Public Hospitals Act and the regulations thereunder. Others, such as the Canadian Council on Hospital Accreditation, may have genuine and appropriate needs for information from patients' records, but access for them is not authorized under legislation. These situations compromise the hospital which releases information notwithstanding legislation which may be prohibitive or ambiguous, and encroaches on the right of the patient to the confidentiality of his or her hospital record. To protect the rights of both the hospital and the patient it is advisable that the governing legislation specify all persons entitled to access and the circumstances under which access is authorized.

*Recommendation:*

55. *That the legislation governing the confidential information maintained by hospitals and health-care facilities designate all persons or groups of persons who may receive or inspect confidential information, as well as the purposes for which their receipt of information is authorized, prohibiting disclosure of or access to information under all other circumstances unless the patient has consented to the disclosure or it is made pursuant to a search warrant, subpoena or order of a court of competent jurisdiction.*

Mental Health/Ontario, the Ontario division of the Canadian Mental Health Association, submitted that disclosure should be permitted only under "narrow legal circumstances" specified in the statute, and proposed that "the legislative exceptions to the general rule requiring consent to release information should provide access to a specified section of the record." Our survey of current policies and procedures in hospitals in Ontario revealed that some hospitals routinely release the entire medical record of the patient to an authorized recipient without limiting their disclosures to the amount and type of information actually required by the recipient. In fact, the patient authorization forms created by some hospitals do not even require that the purpose of the request be specified. The patient's right to privacy is jeopardized whenever the health-care provider releases information which is unnecessary for, or irrelevant to, the purpose for which the disclosure is permitted. Although I agree with the concern reflected in the proposal of Mental Health/Ontario, to legislate precisely which sections of the record may be released to every authorized

recipient is unfeasible. The proper role of the legislation in controlling the amount and type of information disclosed is, rather, to create a general standard of information management, requiring that, whenever release is discretionary, the information manager restrict the information disclosed to that which is reasonably sufficient to accomplish the purpose for which disclosure is permitted. This was also a recommendation of the U.S. Privacy Protection Study Commission in its report, Personal Privacy in an Information Society.

*Recommendation:*

56. *That legislation require hospitals and health-care facilities, when they exercise a discretion to disclose, to limit their disclosure of confidential patient information to the amount and type of information necessary to accomplish the purpose for which the disclosure is authorized.*

During our inquiry we discovered a reluctance on the part of some hospital employees to attempt to verify the identity of an inquirer to ensure his or her authenticity, a reluctance stemming at times from carelessness or, more often, from fear of offending the inquirer. This diffidence partly explains the ease with which private investigators were able to gain access to confidential hospital information without the consent of the patients affected. The policies and procedures dealing with release of patient information should provide for verification of the identity of inquirers.

*Recommendation:*

57. *That hospitals and health-care facilities permit the disclosure of information only to authorized persons whose identity has been properly verified.*

An efficient system for recording the requests for confidential information and the disclosures made in response to these requests should also be maintained. Our survey of Ontario hospitals revealed that many hospitals attach a notation of the release of information from a particular patient's record to that record itself. This control procedure will also be useful to patients gaining access to their own records, as it will indicate those parties who have obtained information concerning the patient.

It would be much easier to monitor hospitals' release procedures and their effectiveness in the protection of personal privacy if logs were to become universal, recording, in one central location, the particulars of the hospital's disclosures of confidential patient-identifiable information. In December, 1977, and January, 1978, respectively, provincial psychiatric hospitals and public hospitals with psychiatric units received a memorandum from the Ministry of Health asking them to maintain a daily log of the release of psychiatric patient information, and to retain it for five years "in order to develop statistics regarding information requests." The memorandum advised the hospitals that the log should set out the following details:

date of request, patient's name and case book number, type of request (e.g. search warrant, subpoena, etc.), disposition of request, date of information sent, initials of person sending information.

There is no reason why the same practice should not be followed with respect to non-psychiatric patients.

Maintaining a brief but full accounting of all disclosures of confidential information allows for monitoring of hospital information release practices by patients, the information manager, and any authorized regulatory bodies. This logging of access to, and disclosure of, confidential information for information management and privacy protection purposes was endorsed by the Australian Law Reform Commission in its Research Paper No. 7: Medical Records, where, at page 83, the following recommendation is found:

Logs of Transactions: Logs should be kept by the information manager in respect of the following matters:

- (a) access by the subject to personal information held about him or her; and
- (b) disclosure of personal information to persons not employed by the collector of the information or for purposes which are incompatible with or not related to the purpose for which the information was collected.

The Research Paper went further and recommended that the hospital should, whenever possible, not only notify the patient of

the disclosure made but also send him or her a copy of the information released:

Notice of Disclosure: Wherever practicable, the fact of any disclosure, a copy of information disclosed, and details concerning all parties involved, should be forwarded to the subject within a reasonable period following such disclosure.

I am not persuaded that it is reasonable to require a hospital or health-care facility, already burdened with the responsibility of releasing information in accordance with the legislation, to assume the onerous task of notifying its former patients of the details of every disclosure. Only when disclosures are made that will probably be of some consequence to the patient (other than an infringement on his privacy) should hospitals, whenever possible, notify the patients of the fact of the disclosures. For example, a report sent to the Workmen's Compensation Board would probably have material consequences for an injured claimant, whereas the random inspection of this patient's record by the Canadian Council on Hospital Accreditation would not. For disclosures which do not call for any notice, the patient can rely on the hospital's recording of any request for information on his record where it should be made easily accessible to him.

#### *Recommendation:*

*58. That legislation governing hospitals and health-care facilities require these establishments to record the particulars of every request for confidential patient information, except for those made by hospital staff members for routine hospital purposes. The access to and disclosure of this information must be logged both in a central registry and on the patient's record itself, the registry being retained separately for an adequate period of time.*

Once a health-care facility makes a disclosure of information under any of the provisions allowing for disclosure without the consent of the patient, its control over that information is lost, and the danger that this information may be redisclosed or used for another purpose without further authorization is always present. An example of unauthorized redisclosure is the case of patient-identifiable information released for use in approved research projects being subsequently published without



the patients' consent. All recipients of confidential health information under such provisions for disclosure should be under an obligation, stated clearly in the legislation, to refrain from redisclosing any confidential information received from a hospital or health-care facility to any person or persons or from using it for any purpose other than those for which the information was given.

*Recommendation:*

59. *That, where confidential patient information maintained by hospitals and health-care facilities is disclosed without the consent of the patient under any of the provisions in the legislation allowing for such disclosure, legislation require that the confidential patient information so disclosed not be further disclosed in identifiable form unless it is required by law, or unless the information is required to relieve an emergency situation affecting the health or safety of any person.*

Patient Consent to Disclosure

Section 48 of Regulation 729, made under The Public Hospitals Act, makes the following general provision for disclosure of health information by a public hospital to a third party with the authorization of the patient:

(1) Subject to subsections 2, 3, 4 and 5, a board shall not permit any person to remove, inspect or receive information from a medical record.

. . . . .

(5) A board may permit,

. . . . .

(c) a person who presents a written request signed by,

(i) the patient,

(ii) where the record is of a former patient, deceased, his personal representative; or

(iii) the parent or guardian of an unmarried patient under eighteen years of age;

. . . . .

to inspect and receive information from a medical record and to be given copies therefrom.

For psychiatric facilities, the disclosure of health information is governed by The Mental Health Act, section 26a of which provides as follows:

(3) The officer in charge and the attending physician in the psychiatric facility in which a clinical record was prepared may examine the clinical record and the officer in charge may disclose or transmit the clinical record to or permit the examination of the clinical record by,

(a) where the patient has attained the age of majority and is mentally competent, any person with the consent of the patient;

(b) where the patient has not attained the age of majority or is not mentally competent, any person with the consent of the nearest relative of the patient;

. . . . .

Any dissemination of patient-identifiable confidential information outside the health-care institution threatens patient privacy. Every time a patient authorizes disclosure by the institution to a third party the patient should be fully aware of the nature of the information to be divulged. The present legislation governing the disclosure of medical information with the consent of the patient fails to provide adequate guidelines respecting the content of an 'informed consent'. In another section of this report I discuss the minimum requirements of an

informed consent. The recommendations found there apply equally to the legislation governing confidential patient information in hospitals and other health-care facilities.

Under the present legislation the hospital board or the officer in charge of a psychiatric facility has a discretion as to whether or not a person with a proper written consent from the patient should be permitted to receive the latter's confidential health information. The discretionary power may help the institutional health-care provider protect the confidentiality of the patient's information if it is exercised to prevent the disclosure of more information than is necessary to fulfill the purpose for which the information is requested, or when it is considered to be injurious to the patient or another to disclose the contents of the record. However, there may be a conflict of interest if the hospital or health-care facility suspects that the patient is authorizing the disclosure of his or her record in order to use the information in a way adverse to the interests of the releasing establishment. Some hospitals refuse to release patient information if they suspect that the information is desired because a civil action against them is contemplated. In my discussion, elsewhere in this report, of access to one's own health information, I recommend that patients be given a legal right of access to their own health information. This would prevent a hospital or health-care facility from withholding information from a patient, subject to an application to a Health Commissioner, or on appeal to the Supreme Court, where the hospital or facility believes that the disclosure of this information would be injurious to the physical or mental health of the patient or of any other person. Similarly, the right of the patient to authorize the disclosure of information to a third person should be subject to the right of the hospital or a facility to withhold information where to disclose it would be injurious to the physical or mental health of the patient or another. However, provided that a right of appeal is given to the institution and that the patient is entitled to have access to his or her own information, I can see no reason why the patient's authorization should not be required to command the respect of the institution.

### Staff Access

Control of staff access to confidential patient information is important to the protection of the privacy of patients both within and beyond the hospital. The primary use of patient health information by hospital personnel is for the purpose of providing co-ordinated diagnostic and treatment services for

patients. Section 26a(3)(c) of The Mental Health Act allows the clinical record to be disclosed to or examined by:

any person employed in or on the staff of the psychiatric facility for the purpose of assessing or treating or assisting in assessing or treating the patient;

In the case of public hospitals, a number of professionals and other hospital employees are involved in the assessment and treatment of patients, and, normally, all of them require access to confidential patient information in the course of their involvement. The legislation governing access to medical record information for health-care purposes appears to be based on the erroneous assumption that the only person caring for a patient in a public hospital is that patient's physician. The only member of the treatment team who may be permitted to "inspect and receive information from a medical record" under section 48(5)(a) of Regulation 729 is the patient's "attending physician". The failure of the present legislation to authorize access by other hospital staff to confidential information for health-care purposes has been the subject of concern on the part of such groups as the Ontario Council of Health's Task Force on Medical Record Keeping, the Ontario Health Record Association, and the Ontario College of Health Record Administrators.

The categories of employees needing access to confidential information for treatment purposes will vary with different types of health-care facilities. Every health-care centre should be permitted to determine which categories of personnel "need to know" some amount of confidential information for health-care purposes. In its 1977 Position Statement entitled Confidentiality of Patient Health Information, the American Medical Record Association recommended that,

Health records shall be available for use within the facility for direct patient care by all authorized personnel as specified by the chief executive officer, and documented in a policy manual.

Access to health record information for routine administrative functions must also be permitted, provided that the employees have been educated with respect to their responsibility to maintain confidentiality. Again, every health-care facility should be made responsible for determining which employees require access for administrative purposes.

Regulation 729 under The Public Hospitals Act requires the hospital board to pass by-laws to provide for various committees and other designated internal auditors to analyse the hospital's clinical procedures and record-keeping practices, but says nothing about authority to disclose patient-identifiable information for these purposes in section 48. One of these internal audit mechanisms required under section 6 of Regulation 729 is the medical advisory committee, which supervises the practice of medicine in the hospital. Other committees contemplated by the Regulation to review and assess the professional performance of the hospital and its compliance with proper standards are described in the following provisions:

6. (1) The board shall pass by-laws that provide for,

. . . . .

(d) the appointment of members of the medical staff, on the recommendation of the medical staff or the election of such members by the medical staff, to,

(i) a credentials committee,

(ii) a records committee,

and, where there are ten or more members on the active medical staff,

(iii) a therapeutic abortion committee, where therapeutic abortions are to be performed,

(iv) an admission and discharge committee, and

(v) except in hospitals for convalescent persons and hospitals for chronically ill persons, a tissue committee or a medical audit and tissue committee,

and that prescribe the duties and powers of such committees;



Section 41 of The Public Hospitals Act provides for the evaluation of the "quality of medical diagnosis, care and treatment provided to the patients and out-patients of the hospital." When designated officers of the medical staff become aware that the care being given to a patient by a member of their medical staff is inadequate (and satisfactory changes are not made promptly by the attending physician), these officers must assume responsibility for "investigating, diagnosing, prescribing for and treating the patient or out-patient" in order to ensure that proper care is given to the patient involved.

These audit committees and "officers of the medical staff" are designated by the legislation to discharge the important function of evaluating the quality of patient care and services provided by the hospital. There is no doubt that these auditors require access to confidential information about patients (who have not authorized this disclosure) in order to carry out their duties of review, evaluation or investigation. Neither The Public Hospitals Act nor The Mental Health Act authorizes disclosure for these purposes.

Since members of the nursing staff require patients' medical records for the assessment of nurses' performance and members of the medical record department need to review medical records in the discharge of their functions, it is unreasonable to limit access for audit and quality control purposes to members of the medical staff of hospitals. In the 1978 Report of the Ontario Council of Health on Medical Record Keeping, it was recommended that section 48 of Regulation 729 be changed to permit access for the purpose of audit, and that access for this purpose not be limited to "member[s] of the medical staff" but be expanded to include "other person[s] authorized by the board." Again, precisely which persons on staff of or employed by a health-care centre "need to know" confidential information for these purposes must be a matter for the administration of each facility to specify in its by-laws.

Internal audits of hospital work performances may eventually result in an employee discipline or grievance hearing at which one of the parties may desire to refer to information in medical records, without the patients' authorization, as relevant evidence. The present legislation governing health-care institutions does not authorize this use of confidential patient information. The American Psychiatric Association's Model Law on Confidentiality of Health and Social Service Records makes the following provision for hearings of this kind:

In the course of any disciplinary or dismissal actions against such employees, confidential information shall not be used except to the extent necessary to comply with principles of fair notice and hearing, and patient/client identifiers shall be removed from any such information prior to its use in such proceedings.

There is no reason why patient identifiers should not be removed before patient information is used in discipline or grievance hearings, audit reports, or minutes of hospital committee meetings at which the information has been used.

Access to patients' records for the purposes of research and teaching is now authorized by Regulation 729 under The Public Hospitals Act and The Mental Health Act, although the language of these two pieces of legislation is very different. Under section 48(5)(d) of Regulation 729 "a member of the medical staff" may be permitted access "for teaching purposes, or scientific research that has been approved by the medical-staff advisory committee", whereas by section 26a(3)(f) of The Mental Health Act, the examination of the clinical record by "a person for the purpose of research, academic pursuits or the compilation of statistical data" may be permitted, a much wider provision. The subject of access for research purposes is dealt with elsewhere in this report, but with respect to in-house access, the question is whether or not employees of a public hospital who are not members of the medical staff--for example, students, research assistants, nurses or other health-care professionals--may have a legitimate need to have access to patient-identifiable health information for research or academic purposes which the legislation should permit. The evidence at our hearings makes it clear that access by these employees for research purposes already exists in fact in many public hospitals despite the language of Regulation 729. At our McMaster University hearings, Professor Michael Gent, chairman of the Department of Clinical Epidemiology and Biostatistics at that university gave this description of what happens in the real world.

MR. COMMISSIONER: It seems to me that there is an increasing practice to find people being allowed access to information in hospitals records who are not physicians, but for some reason or other are given access...

PROFESSOR GENT: It's probably even worse than that, you see, because in our

enthusiasm and ignorance I'm sure all of us, I know that all of us are involved in studies which contravene that particular regulation. For example, if you are into a clinical trial in the chronic care unit, let's say, and suppose...and this is actually a real situation...suppose in fact that what you are trying to do is to identify patients who come into the chronic care unit who have unstable angina. The idea being that once you identify those patients, you then formally seek informed consent and ask them if they will take part in the prospective randomized trial.

Now this is a current...it happens everywhere. What would happen is that those patients are not screened out by a physician, by the cardiologist, because he wouldn't have time. What would happen in practice is all the records of every patient who comes into the chronic care unit would be screened by a nurse practitioner. She would go through a process eliminating out non-specific pain and ruling out infarctions, so that one eventually gets down to a group who through her particular skill she is pretty sure they have angina. She will then get a cardiologist in who will then check her records and confirm them.

But at that point in time, she has already been through all the records and picked out those patients. Again, we don't ever get any hue and cry from the patient because this is the setting, you see, where the patients I think were not alarmed by the fact that they had been picked up from somebody looking at their records, because in this case they are in there for an acute attack anyway.

But in principle that's no different from the patient who gets picked up through some much more remote record system, who then get addressed and say, how did you find out. Now, you know, if events are distant in time, the event concerned, yet really the principle is no different.

With respect to access to the record for purposes of education, the Ontario Hospital Association made this observation in its brief:

There is currently no specific permission given in section 48 of Regulation 729 for access by students from community colleges to medical information. However, students in the health professions have always had access to confidential information about individual patients as a normal part of the process of gaining experience and becoming a recognized health care worker in the hospital environment.

Internal statistical compilation of information abstracted from the medical record, which is permissible under section 26a(3)(f) of The Mental Health Act, is another use of confidential information that is not authorized under Regulation 729. Nevertheless, hospitals often analyze their use of facilities, equipment, services, personnel and financial resources through statistics abstracted from medical records, usually employing members of their medical record departments to do so. The legislation should permit access for this purpose provided that every hospital or health-care facility is required to specify in its by-laws the categories of employees who will be authorized recipients for the purpose.

The legislation must be wide enough to allow internal access for all appropriate purposes, while being as specific as possible to limit unnecessary disclosure. The U.S. Bill H.R. 5935, the "Federal Privacy of Medical Information Act", contains the following provision:

121. (a) A medical care facility may disclose medical information it maintains about a patient, without the [patient's] authorization described in section 115(a), if the disclosure is to an employee...of the facility who has a need for the medical information in the performance of his duties.

This section provides access for all of the purposes discussed above, but since disclosure for some uses, for example, internal audit or research, is not something that patients would necessarily expect, it is, in my view, too broad. In the brief of the Canadian Civil Liberties Association, on the other hand, the submission was made that in-house access that exceeds patient expectations should require consent:

Inevitably, when patients submit themselves to the care of particular doctors, they must expect that they will be the subject of certain communications between those doctors and other personnel involved in the health care system--nurses, receptionists, orderlies, other doctors, etc. So long as the communication is necessary to the diagnosis, treatment, care, and recovery of that for which the patient sought medical assistance, we would find it difficult to object. To whatever extent, however, communications about the patient exceeded what might be called the patient's reasonable expectations, the law should require a specific consent. Thus, an unexpected multidisciplinary conference concerning a problem of which the patient is unaware or a disclosure to a research worker--both of which identify the patient--should be unlawful without the patient's specific consent.

I am of the opinion that all general categories of authorized employee access should be specified in the legislation, both to inform patients as to the uses to which their confidential information can be put and to prevent inappropriate, unauthorized uses by the facility. Since it would be impractical to specify categories of employees who may have access for each of the authorized purposes in the legislation, the legislation must require every hospital and health-care facility to determine which members of its staff "need to know" information for each of these purposes and to pass by-laws expressing the result.

*Recommendation:*

60. *That legislation permit access to confidential information within hospitals and health-care facilities for the purposes of patient assessment or treatment, internal administration, audit and quality control, research, statistical compilation, and education but only to those staff members whose access has been specifically approved by the respective boards and formally designated in their by-laws.*

Earlier in this discussion I pointed out how confidential information is often indiscriminately disseminated within the



institution, providing hospital employees with more sensitive, patient-identifiable information than they "need to know" in the performance of their duties. The operating room schedule is a good example of unrestricted disclosure. Evidence was given that it is copied in some hospitals more than 50 times for wide internal circulation, while often only 10 per cent of the confidential information which it contains actually applies to the employees in the ward or department in which it is posted.

Limiting the amount and type of information disclosed to designated recipients for authorized purposes is made easier by the use of a computer which can be programmed to display specific types and amounts of data to different categories of employee users and to hold back other information which is inappropriate or unnecessary for their purposes. Of all hospitals in Ontario, York Central Hospital's use of computers is probably the most advanced. At our hearings, its assistant executive director, J. H. Flint, described the effect that the employment of the computer had on controlling the dissemination of information within that hospital:

A bi-product of introducing the computer system was a conscious effort to reduce the amount of sensitive paperwork that flows through a hospital. Do all these staff categories require a copy of the Operating Room schedule, for example? This type of review made us more aware that staff who required only several pieces of information were receiving a standard report that made not only the required information available but also a great deal of additional information not required by that employee to do their job. We made changes in our manual system so that security and confidentiality in our new computerized environment would be much higher than with the previous manual system.

. . . . .

One of our methods of ensuring "the appropriate user" is to examine the need for information and eliminating the "nice to know" information inadvertently made available. At times we are so restrictive with information in the computer system that we have not identified a user with real need for access.

With or without computerization, it is essential to undertake a comprehensive evaluation of the quantity and quality of information required by every staff member or employee in the performance of his or her duties. Only by doing so can affirmative procedures be adopted by which limitations on access can be enforced.

I have made reference to the desirability of ensuring that patient information not be disclosed unless the identity of the recipient is properly verified. This means determining that the employee is who he or she says he or she is, something that can be confirmed through the use of identification tags, a safeguard which I have already recommended in another section of this report, or through the use of identification codes for computer purposes. The Ontario Hospital Association, the Registered Nurses Association, the Canadian Health Record Association and several individual hospitals all voiced concern about the extent to which physicians have access in hospitals to information about other physicians' patients, which they do not require in the performance of their duties. Some nurses, clerks, receptionists, and health record administrators are impressed, if not intimidated, by a physician's professional status, and are reluctant to question his or her right of access to any patient's material. For example, the medical record administrator at St. Thomas-Elgin General Hospital, gave this evidence at one of our hearings:

Q. ...The question is, when a physician comes in, he asks to see the file of a patient who has already been discharged. The file card would indicate that he wasn't a treating physician. Would you let him have the file?

A. I probably would.

MR. COMMISSIONER: Are you not always going to make the assumption that he...wouldn't be asking unless he were professionally involved?

A. Right. Right.

MR. COMMISSIONER: You always make that assumption? If Doctor Smith, who is known to you to be a member of the staff, should phone you and say Miss Tolgyes, I will be in after hours. Would you mind getting out the file of Mrs. James and putting it in my box,

I want to have a look at it. You would do it for him, wouldn't you?...

A. Yes, I would. Yes.

Obviously the patient's privacy is compromised by any failure on the part of a record custodian to verify the propriety of the disclosure, but the designation in hospital procedure guidelines and by-laws of authorized personnel along with the logging of all non-routine disclosures should assist in controlling internal hospital access.

### Hospital Board Members

From a discussion of access by hospital employees to patient information they need to be able to discharge their responsibilities, I move to the related but separate issue of the right of hospital board members to access to confidential patient information kept in their hospitals. Board members are trustees or governors, directors of the hospital as a corporate entity, and are not employees of their hospitals. The question is whether access to patient records is necessary for the performance of the functions of a hospital board which, according to sections 2 and 3 of Regulation 729 under The Public Hospitals Act, are to govern and manage the hospital, enforce The Public Hospitals Act, Regulation 729, and the by-laws of the hospital.

This issue was graphically brought to our attention by Jon R. Skafel, executive director of the St. Thomas-Elgin General Hospital in St. Thomas. He wrote to us to say that four new governors "represent[ing] an anti-abortion viewpoint" had been elected to his hospital's 16 member board of governors in June, 1978, and were now requesting confidential information about every abortion application made to the therapeutic abortion committee of the St. Thomas-Elgin General Hospital. The platform on which the four new governors had run for election to the board was based on a philosophical opposition to abortion and an intention "to question, review and tighten the hospital's abortion policy." Mr. Skafel was concerned about the confidentiality of his hospital's medical records if it turned out that the board of governors had the legal authority to "see and/or obtain information from this Hospital's medical records", a right claimed on behalf of the anti-abortion board members. The solicitors for the St. Thomas-Elgin General Hospital had given an opinion to the effect that the governors had no such right to information from the medical records.

The question raised by these opposing points of view became the subject of one of our public hearings. The principal question was the right of the board to access to patient health information without the consent or knowledge of the patients concerned. Subsidiary questions included the following: Is existing legislation adequate to answer the main question? What is the nature of the board's responsibility for the quality of health care provided to the community? What kind of information does a hospital board need to be able to discharge that responsibility? At the hearing, Dr. Adrian Borre, president of the St. Thomas-Elgin General Hospital medical staff, described the three different levels of authority at his hospital involved with this issue: the therapeutic abortion committee, the medical advisory committee and the board of governors. The procedure for obtaining permission for a therapeutic abortion begins when a patient's physician makes a submission to the therapeutic abortion committee asserting that there is a medical necessity for his or her patient to have a therapeutic abortion. A written statement submitted by Dr. Borre, and entered in evidence as an exhibit at the hearings, sets out the procedure that is followed:

The Therapeutic Abortion Committee shall

- (a) meet, as necessary, to consider the written request of a member of the medical staff to the administrator for a certificate for a therapeutic abortion as referred to in the Criminal Code of Canada;
- (b) consider information relating to the pregnancy of a female person who is a patient of such member of the medical staff of the hospital with reference to the effect the continuance of that pregnancy may have on the life or health of such female person;
- (c) request such additional information as it deems advisable and may adjourn any meeting for this purpose;
- (d) complete, in each case, a certificate stating that in its opinion the continuation of the pregnancy would or would not be likely to endanger the life or health of such female person, provided that no certificate may be completed

unless approved by the majority of the members of the Committee, and no member may vote unless present at the meeting; and

- (e) ensure that a copy of such certificate is given to the member of the medical staff requesting the opinion.

The administrator shall supply copies of such certificates as required for hospital purposes.

In practice one copy of the certificate is sent to each of the two referring physicians, one to the administrator, one, in an envelope, to the operating room supervisor (which becomes the patient's chart copy) and one is kept with the therapeutic abortion committee's report in an unlocked filing cabinet in the medical record department, separate from the ordinary medical records. Minutes dictated by the chairman of the therapeutic abortion committee, which summarize all business dealt with at the meetings, are kept in another file in the medical record department.

The medical advisory committee is the committee that oversees the medical staff, the practice of medicine, and the quality of medical care provided in the hospital. A monthly report is made to this committee by the therapeutic abortion committee. This report contains the number of applications which have been made for abortion, the number granted or accepted, the number rejected and the number of abortions actually performed. Of these statistics, one, the number of abortions performed by the hospital that month, is passed on by the medical advisory committee to the board of governors as part of its monthly statistical report. The board is not told how many requests for a therapeutic abortion are refused by the therapeutic abortion committee.

The four new anti-abortion governors thought that the board should be given more information than this. They wanted the board to be told the criteria being used by the therapeutic abortion committee in deciding whether or not a woman's request for an abortion should be granted. One of these governors, Mary Anne Evans, testified at our hearings that she suspected that, in its granting of permission for abortions, the therapeutic abortion committee had been using criteria that were an abuse of the criterion for the procurement of miscarriage set out in section 251(4)(c) of the Criminal Code R.S.C. 1970, chapter C-34, that is, that "the continuation of the pregnancy of such



female person would or would be likely to endanger her life or health." To demonstrate this abuse, Mrs. Evans wanted the board of governors to be supplied with information about all of the requests for abortion. This would enable the board to set a new policy with a more stringent set of guidelines for the therapeutic abortion committee to follow. Accordingly, she and two other anti-abortion board members submitted a brief to the full board in September, 1978, recommending the information they thought the board should be given for every applicant for abortion whose case was being considered by the hospital's therapeutic abortion committee. The recommendation read as follows:

### Recommendation 3

#### APPLICATIONS AND REPORTS

- (A) An abortion APPLICATION to be submitted to the Therapeutic Abortion Committee should include:
- 1) name and address of the hospital
  - 2) date
  - 3) patient name
  - 4) age of pregnant woman
  - 5) marital status
  - 6) number of previous pregnancies
  - 7) number of living children
  - 8) number of previous induced abortions
  - 9) date of last induced abortion
  - 10) date of last live birth
  - 11) result of amniocentesis, if applicable
  - 12) method of contraception at time of conception
  - 13) type and result of pregnancy test
  - 14) type of abortion procedure recommended
  - 15) type of family planning recommended
  - 16) type of additional counselling given
  - 17) medical reasons for inability of pregnant woman to carry pregnancy to term
  - 18) a copy of signed consent form
  - 19) the name of the physician(s) requesting the abortion
- (B) An individual abortion REPORT for each induced abortion requested should consist of the above information stamped

"granted" or "denied". The REPORT should not contain the name of the pregnant woman or a copy of the signed consent form.

- (C) ALL abortion REPORTS should be submitted to the Medical Advisory Board on a monthly basis.
- (D) A copy of all abortion REPORTS should be made a part of the monthly report of the medical staff to the Board of Governors.
- (E) The annual medical report to the members of the Corporation should include the number of abortions requested, the number of abortions performed and the number of abortions denied. [emphasis added]

Although the authors of the brief recommended that the board receive a great deal of information on all women applying for abortions to the hospital, they did not ask that the applicants' names or the consent forms identifying them be included in the board's version of the reports. One might have thought that the omission of the patients' names would make it impossible to identify them. Mr. Skafel denied that this was so. According to him the small and insular nature of the St. Thomas-Elgin community would result in the recognition of many of the subjects of the reports even without the inclusion of their names. In his testimony at the hearing he put it this way:

I think it's partly because St. Thomas-Elgin is not a large community and in a hospital that has approximately six hundred employees in it, it is very possible to deduce from information that does not have the name on it who a patient is. You may not know this patient, but you might know the next one.

Mrs. Evans did not agree that an unnamed patient could often be identified from the other 17 particulars set out in the proposed abortion report. She added that she was not at all interested in learning who was having abortions. This was her opinion:

I think it would be very difficult in a community that serves fifty-two thousand people, a great number of whom would be women between the ages of thirteen and

forty-five, and the services of our hospital are not prohibited to anyone. So...I doubt very much whether I would recognize a friend of mine as far as those particular things are concerned. I am really not interested at all in who is having abortions. I perceive my responsibility to be the why.

Mrs. Evans thought that if the board of governors were given 17 of the 19 listed particulars about each applicant, its members would be able to deduce how loosely the therapeutic abortion committee applied the criterion for therapeutic abortions set out in the Criminal Code, that is, that the continuation of the pregnancy posed at least a likely danger to the woman's life or health. This information, she felt, was necessary if she was to discharge her responsibility as a board member to monitor the hospital's compliance with the abortion law.

When, in response to the brief, concern was expressed about the threat to the confidentiality of information in the patients' medical records which the recommendation would cause, Mrs. Evans changed the form of her request. Still determined to learn the reasons for the granting of requests for therapeutic abortions, she asked that the board be given the number of abortions applied for each month, the number of applications rejected by the therapeutic abortion committee, and an analysis of the number of abortions granted according to the reason for approval (e.g. the number granted for "social" reasons, for "economic" reasons, for "eugenic" reasons, etc.). The request for statistics also met with disapproval. Dr. Borre explained that these statistics would not faithfully reflect the number of abortion requests rejected because most are turned down at the general practitioner stage, that is, before they ever reach the therapeutic abortion committee. Put another way, it was Dr. Borre's opinion that the chances are very good that there are valid grounds for any request that reaches the committee. The true incidence of successful applications for abortion would not be disclosed by the number of abortion requests refused by the committee. Mr. Skafel felt that the statistics requested could readily be misinterpreted by such groups as the anti-abortionists who might want to use them to "serve their own ends".

Dr. Borre and Mr. Skafel added that the statistics asked for would be compiled from personal medical record information, "private information between the patient and the patient's doctor," and that presenting the figures to the board would therefore constitute a breach of confidentiality. I am not persuaded that, provided the reporting period were sufficiently

long, there would result a breach of confidentiality if the board were to be provided with the number of therapeutic abortions (or indeed other kinds of surgical or other procedures as well) performed in the last reporting period, the reasons for the performance, and the number of requests for abortion refused. On the other hand, given the current state of the law, I find it difficult to believe that the report would show any other reason for the performance of the therapeutic abortions than that continuation of the pregnancies would or would be likely to endanger the life or health of the patients.

It was also said that this information is unnecessary for, and irrelevant to, the functions of the board. The functions and responsibilities of a board of a public hospital in Ontario are thus brought into question. By virtue of Section 2(1) of Regulation 729 under The Public Hospitals Act, a hospital "shall be governed and managed" by its board, most of whose members are non-physicians elected or appointed from the community. Section 3 of the Regulation provides that "the board is responsible for the enforcement of the Act, this Regulation and the by-laws of the hospital." The board is made responsible by the legislation for developing policies, passing by-laws, appointing committees, and ensuring the establishment and execution of hospital procedures. Put in a few words, the board has the ultimate responsibility for what goes on in its hospital. "The Board of Governors of a public hospital is entrusted by its community with the responsibility of providing a program of health care tailored to the particular needs of that community." That statement, originally made by the Hospital Appeal Board, has been quoted with approval in several decisions of our courts and is one which accurately sums up my perception of a board's purpose. But to say that does not determine the information the members of the board require to enable them to discharge their responsibilities. Indeed, under existing legislation it is not clear what the extent of the board's access to information is. Section 11 of The Public Hospitals Act provides that "the medical record compiled in a hospital for a patient or an out-patient is the property of the hospital and shall be kept in the custody of the administrator." It is arguable that since the hospital acts through its board of trustees or board of governors, with ownership of the records residing in the hospital, the corporate entity, the trustees or governors have a right of access to them. The scheme of the legislation may give rise to an inference that the board, and therefore its members, are entitled to extensive information about patients because of the reports made to the board by the hospital's various medical committees.

The board is obliged to take measures to protect the information in the records which it owns and to ensure that only persons authorized to have information from the records are given access to them. Section 48(1) of Regulation 729 under The Public Hospitals Act says that, "subject to subsections 2, 3, 4 and 5, a board shall not permit any person to remove, inspect or receive information from a medical record." Although no express provision exists providing for access to this medical information by the board, it may be reasonable to infer a right in the board to inspect medical records from its duty to prevent some persons from having access to them and its right to permit others to see them. This question was the subject of a recent pronouncement in a judgment of the Supreme Court of Ontario. The pronouncement was not an essential part of the judgment but since it was a considered statement it is entitled to be treated with great respect. In Re General Accident Assurance Company of Canada and Sunnybrook Hospital (1979), 23 O.R. (2d) 513, at p.516, Mr. Justice Carruthers gave section 48(1) of Regulation 729 the following interpretation:

The interpretation of the term "any person" contained in s.48(1) of Regulation 729 which counsel for the respondent hospital has urged upon me is too restrictive, in my view. His interpretation would, in my opinion, lead to the conclusion that, with the exception of those individuals who are specifically designated by the provisions of s.48, only the board as a whole could examine a patient's medical record, and an individual member of the board, although acting within the scope of his duties, could not. Furthermore, the superintendent or administrator of a public hospital, on this basis, could not examine a patient's medical record for the purpose of carrying out his or her duties. This situation hardly seems reasonable when you consider that the regulation itself permits the superintendent or administrator of another hospital, simply by making a written request, to inspect or receive information from and be given copies of that patient's medical record.

I believe that this statement reflects the current state of the law. Individual members of the hospital's board, then, are entitled to examine patients' medical records when carrying out their responsibilities. But what of the future? Should they continue to be so entitled?



I put this question to persons and organizations appearing at our policy hearings whose views I thought might be helpful. They included those attending the St. Thomas-Elgin General Hospital hearing as well as the Ontario Hospital Association, the Canadian Civil Liberties Association and the Canadian and Ontario Health Record Associations. There was a consensus that a member of the board had to have enough information to know what was happening within the hospital, to be well informed of the basis on which judgments were being made in the hospital and, generally, had to know anything that might affect policy making decisions. This is how the Canadian Civil Liberties Association put the matter:

In our view, the law should ensure a sufficient flow of information to enable these boards and, indeed the entire public, to know and understand by what policies the medical decisions are being governed. For the board this would be necessary to the performance of its administrative, managerial, and policy making functions. For the public, this would be necessary to the exercise of its ultimate right of scrutiny and review.

With relation to therapeutic abortions, I interpret this position to mean that the members of the board should have enough information to know and understand the real basis on which the therapeutic abortion committee's decisions are made. This means that the members of the board should be given sufficient statistical, aggregated, non-identifiable information to allow them to evaluate the standards of health care provided in their hospital. The idea that the board members should inspect identifiable information from patients' medical records met with disapproval. Persons with extensive experience as hospital trustees or governors said that they had never required identifiable information from the medical records to be able to carry out their duties.

Professor John Wevers, president of the Ontario Hospital Association expressed the following opinion at our policy hearing:

MR. COMMISSIONER: What I am asking is, does the OHA or its member hospitals have a view about the propriety of any system of hospital regulation which would permit lay trustees or directors, on demand or in the discharge of their duties as trustees, to

have access to an individual patient's records or to individual patients' records?

PROF. WEVERS: Well as a trustee who has been a trustee for quite a number of years, I can't conceivably think of any kind of situation in which it would become necessary for me to examine any kind of medical record. I just don't see the relevance of this. I see no reason why it would become necessary.

. . . . .

I am frankly appalled at even the notion that I would have a right as a hospital trustee, or consider it to be my right, to invade what seems to me to be the privacy of an individual.

To determine whether there were occasions when this type of access might be relevant, I put hypothetical questions to those present at our hearings. I asked Dr. Borre at the St. Thomas-Elgin General Hospital hearing how, if I were a suspicious hospital board trustee, I could find out how up-to-date the medical staff's procedures were. Dr. Borre described the internal and external networks of checks and balances available to board members under the public hospital system in Ontario. Here is our exchange:

MR. COMMISSIONER: I want to test whether or not they are carrying that out. I want to test whether or not the physicians in my hospital are physicians who have kept up to date on developments in the field.

A. You can and may. You carry that out two ways. Number one, you can meet with them and talk about it. That's part of a board's prerogative. Number two, you have your set up of committees within the hospital to determine that is indeed carrying out.

In other words, you have your audit committees, you have your credentials committees. These are all set out in your hospital by-laws, The Public Hospitals Act, that are surveying for you a review of the doctors that they are indeed carrying on the best

competent treatment within your hospital. You would then have the medical advisory to oversee all of those.

MR. COMMISSIONER: But I am concerned about the possibility that, in the hypothetical hospital we are talking about, the credentials committee and the medical advisory committee are themselves, or because they themselves haven't kept up to date, are protecting those who aren't up to date.

A. You have two other reviews. Number one, you have The College of Physicians and Surgeons which are dedicated to patient care and are a disciplinary body of our profession and therefore you can complain to them....

MR. COMMISSIONER: Oh, I have no basis for a complaint.

A. Oh, yes.

MR. COMMISSIONER: Not until I find out the answers to these questions.

A. Oh, yes. You have that. Plus also every hospital has an accreditation committee which is responsible to the board to prove that the medical staff is doing its best job. That committee comes impartially and rates the hospital, decides indeed whether it is carrying on better practice.

MR. COMMISSIONER: That's voluntary.

A. Yes.

MR. COMMISSIONER: They are not required to belong, to be subject to the Canadian Council.

A. I agree with that, but indeed in actual fact any board has that option to demand that if it so wishes.

MR. COMMISSIONER: You are thinking of a hospital with a reasonably large staff, but

we do have public hospitals in Ontario with very small, with maybe...fewer than five physicians, don't we?

A. Yes.

MR. COMMISSIONER: Isn't it possible that in...as small a community as that, nobody wants to make any kind of allegation about the competence or quality of another person because of the small number of persons and because of the fact that it will be clear where the accusation came from and so on?

A. That may be so in theory, sir, but I think in actual practice that isn't so in Ontario.

Professor Wevers, R. Alan Hay and Dr. J. D. Galloway, of the Ontario Hospital Association, agreed with Dr. Borre that these internal hospital committees and external bodies are the appropriate mechanisms by which the boards can ensure the quality of care in the hospital without the need to resort to direct access to identifiable patient medical information:

MR. HAY: They can have access to outside opinion. This is why we have associations and why we work with The College of Physicians and Surgeons and why they have access to outsiders who can come in and advise the board. This is, in my view, the strength of the lay system. It's not that they know the medical records, but they know when something doesn't make sense and they have an obligation to the community to pursue it further, but not to get the records.

The concern of lay trustees or governors whose boards are legally responsible for conduct and actions which they feel less than fully confident to judge professionally is reflected in the following comment:

PROF. WEVERS: I realize Mister Commissioner, that the board is legally responsible for everything that happens in the hospital, including the conduct of the medical profession to whom it grants privileges. And this is one of the, well one of these tensions in life, contradictions in life that

one is legally responsible for that which one is not really professionally competent to judge. But this is also I think one of the strengths of the democratic institution where the public is legally responsible and in some way difficult, in fact I think impossible to define legally, does in a sense have control over what happens. But I should be really quite unhappy if this were interpreted that I as chairman of a board would have a right to ask for release of medical records to me. In a sense, I must find other ways of examining the quality control, in my judgment.

It is important to appreciate that the creation of policy with respect to medical and health matters is different from making medical decisions, and no hospital board can abdicate its responsibility and unquestioningly defer to medical persons when the former is involved. With increasing frequency, social and ethical problems are today intruding in decision-making areas previously thought to be within the exclusive jurisdiction of medically qualified persons. These problems require the contribution and scrutiny of the public through the lay boards of governors or trustees. A hospital, after all, is more than a place where physicians and surgeons practise medicine and surgery. It serves the health, not simply medical, needs of, and must be responsible to, its community. If this were not so there would be no need for lay hospital boards.

Although it was not suggested that hospital board members, who are not physicians, are free to communicate private patient information to the outside world or to use it for their own private, as opposed to their hospital, purposes, it has been pointed out that there exists no express duty on hospital trustees or governors to maintain the confidentiality of information about patients which comes to their attention in the course of their work. Surely it is beyond controversy that there should exist a legally imposed obligation of confidentiality on hospital trustees or governors no less stringent than that binding on hospital employees.

In my introduction I pointed out that I did not interpret my terms of reference as requiring me to become involved in the litigation process. I must, nevertheless, say a few words with relation to the right of the hospital board to make information available to its lawyers or liability insurers when a patient or former patient makes a claim or starts an action against a hospital arising out of his or her treatment in the hospital.



Elsewhere I deal with the right of that patient to his or her own medical information in these same circumstances. The question of the hospital board's right was the subject of the decision of Mr. Justice Carruthers in Re General Accident Assurance Company of Canada and Sunnybrook Hospital, already referred to. It was held in that case that the board's duties and responsibilities in the government and management of the hospital "include the dealing with, or defending of claims or actions made or brought against a hospital." In order to prepare a defence, the board of the hospital must familiarize itself with the relevant circumstances and this involves obtaining the assistance of its agents, its insurer and lawyers. Accordingly, the claimant's medical record must be made available. If this is a technical breach of the patient's privacy, the patient must, where he or she complains of the treatment provided by the hospital, be deemed to authorize the hospital to permit inspection of the chart to its insurer or lawyer to the extent that that is necessary to protect itself from the claim. Simple justice demands no less. But it should be understood that this is one of the exceptional situations in which the board or its agents should have access to the patient's medical record.

The Ontario Hospital Association's brief had this to say about the rule as opposed to the exception:

The Ontario Hospital Association recognizes that the directors of hospital corporations must have access to any and all information within the hospital to the extent required to meet the statutory responsibility of managing the affairs of the corporation. OHA does not consider it either necessary or proper, however, for directors to seek or be given access to medical record information about a specific patient, or to medical information through which the identity of a patient would become known to them.

I agree that the board members ought not to be given access to confidential patient information unless that is essential in the discharge of their duties. As I have indicated, some of a board's responsibilities would be impossible to discharge if it were to be deprived absolutely of this source of information. The passage quoted from the brief of the Ontario Hospital Association takes too narrow a view of the duties and functions of hospital boards which, to repeat, are to provide their communities with responsible and accountable programmes of health care appropriate for their communities and to govern and manage

their hospitals to this end. For most of its information, a board must rely on its medical staff and committees but one can envisage exceptional situations in which a board may have to look beyond this normal source and inspect what medical staff members of the hospitals have recorded in a patient's or in patients' chart or charts. For this reason I cannot recommend an absolute prohibition against access to patient charts on the part of the board of a hospital. This point is not overlooked in the brief of the Ontario Hospital Association:

At the same time it will be recognized that a broad legal proscription against access by hospital directors to medical record information could unnecessarily hamper legitimate and desirable involvement.

The existing legislative scheme is in need of change. Some of the questions which I have discussed and which are either not the subject of treatment at all or of appropriate treatment should be given express answers. A hospital board's right to any statistical and non-identifiable information which it requires to be able to discharge its responsibilities must be spelled out. The Public Hospitals Act should be amended to provide for access by the boards and their agents, where appropriate, to patient information where such access is essential to the boards in their government and management of their hospitals as, for example, in the defence of actions brought by patients in connection with their care. This right should not be one to be exercised at the whim of an individual board member or of individual board members but only after deliberation and a corporate decision by the board. In this connection I refer to the American Hospital Association's pamphlet Hospital Medical Records: Guidelines for their Use and the Release of Information and the following passage which recommends that board access to patient information be through the administrator:

...Requests by board members for use of the medical records or release of information therein are channeled to the hospital administrator. It is the administrator's responsibility to determine the justification for such requests and decide whether to grant or deny access to the medical records. On rare occasions, a hospital trustee may have the legal right and, indeed, the obligation to examine medical records if his responsibilities of trusteeship are involved.

I endorse this position.

## *Recommendations:*

61. That where a claim is made or an action is brought against a hospital by a patient or former patient in respect of the care given to the patient, the hospital board, through the administrator, be permitted to disclose the contents of that patient's medical record to the hospital's liability insurer and solicitors to enable them to ascertain the circumstances giving rise to the claim or action and, where appropriate, defend the hospital's position.
62. That a hospital board's right to such statistical and non-identifiable information as it requires in order properly to discharge its obligation to govern and manage its hospital be given express statutory recognition.
63. That in exceptional cases, where it is essential for the discharge of their duties, members of hospital boards be permitted to have access to patients' medical records. Requests for access should be made to the administrator, who must obtain the approval of the board before permitting the access.
64. That the obligation of confidentiality binding on hospital employees be extended to members of hospital boards.

## Service Organizations

Provision must be made for routine hospital tasks that deal with identifiable health information but are not performed by hospital employees. Because of the expense, equipment or training involved, hospitals often contract out certain jobs to individuals and service organizations. As the Canadian Health Record Association explained in its brief,

A service organization in this context refers to a firm or corporation, government or private, which will receive health data for the purposes of electronic data

processing, medical transcription, micro-filming, etc., or for transporting or transmittal, i.e. a courier or delivery service.

Increasingly, hospitals send their medical records to outside agencies for microfilming, to give just one example. This practice is not provided for in the present legislation governing the confidentiality of patient information in hospitals and other health-care facilities. For reasons of finance and efficiency, hospitals may have a real need to transmit patient information to outside agencies for servicing but there must be precautions taken to ensure that the patients' privacy will be properly safeguarded by the service agencies. The evidence is that these organizations are usually quite stringent in their standards of information management, although some lapses have occurred.

In its brief, the Canadian Health Record Association proposed that the contract between the hospital and the service organization be required to include the responsibilities of the latter with regard to patient information handling, security, release, access and destruction, as well as the penalty which any violation of these responsibilities would bring to the service organization:

There shall be a written contract or letter of intent, developed with legal advice if necessary, with the service organization wherein the organization states:

- i. security of health information will be ensured;
- ii. the methods by which the information will be handled and transported;
- iii. the number and types of individuals who will have access to the information, limiting these to those persons directly involved in processing;
- iv. that information will not be released to any individual(s) other than the institution.
- v. any penalty for violation of security and breach of confidentiality;

- vi. the means of disposal of the original documentation when the service has been completed.

I have already recommended that, where a hospital's or health-care facility's confidential patient information is disclosed under any of the legislative provisions allowing for such disclosure, the legislation require that the information not be redisclosed by the recipient unless required by law or in an emergency situation. It would also be advisable that a hospital or health-care facility utilizing a service agency include specific provisions for record management in the legal agreement between the two parties.

*Recommendation:*

65. *That legislation permit the hospital or health-care facility to release patient information to an outside service organization without patient authorization, provided that the agreement between the parties provides for regulation of access to, release, handling, transmittal, security and destruction of identifiable patient information.*

### Inter-Hospital Communication

Inter-hospital communication is a regular and often necessary part of patient health care. A patient may be transferred from one facility to another. For example, it is sometimes necessary for a hospital to transfer a patient to another hospital because the transferring hospital is not equipped to provide the necessary services. A hospital may transfer a patient to another hospital temporarily for a specialized service, treatment, or diagnostic procedure. Patients are also transferred from general hospitals to other health-care facilities such as convalescent hospitals, rehabilitation hospitals, chronic care hospitals, and nursing homes.

When transfers of these kinds occur the question arises whether or not the original hospital should be permitted to release confidential health information, without the express consent of the patient, to the health-care facility to which the patient is transferred. The purpose of forwarding the information to the second centre is obvious; it facilitates continuing care of high quality.



In the legislation presently governing these facilities the only provision for the automatic transfer of confidential health information, without formal request or patient authorization, is found in section 91(4)(c) of O. Reg. 196/72 under The Nursing Homes Act, 1972, whereby "the administrator of another nursing home to which the resident has been transferred" may be permitted to inspect, receive information and be given copies from the resident's medical or drug record.

Neither The Public Hospitals Act nor The Mental Health Act specifically mentions transfer in their relevant release provisions, but this type of inter-hospital (or inter-facility) exchange is covered under much broader provisions. For example, section 48 of Regulation 729 under The Public Hospitals Act contains this provision:

(5) A board may permit,

. . . . .

(b) the administrator of another hospital who makes a written request to the administrator;

. . . . .

to inspect and receive information from a medical record and to be given copies therefrom.

The administrator of the 'other hospital' need not be receiving a transferred patient from the first; in fact, it is not even necessary that the second hospital be treating a patient for it to be entitled (with the permission of the board of the first hospital) to receive confidential information without that patient's consent. What is required is that the recipient be another "hospital" (as defined by The Public Hospitals Act) and not any other type of health-care facility.

Section 26a(3)(d) of The Mental Health Act is more distinctly formulated, although it also applies to situations beyond the direct transfer of a patient from one facility to another:

...the officer in charge may disclose or transmit the clinical record to or permit the examination of the clinical record by,

. . . . .

- (d) the chief executive officer of a health facility that is currently involved in the direct health care of the patient upon the written request of the chief executive officer to the officer in charge;

In this case the receiver need not be generically identical to the discloser; in other words the officer in charge of a psychiatric facility is permitted to reveal the record to the chief executive officer of a "health facility" (which is not defined). This provision does require that the receiving "health facility" be "involved in the direct health care of the patient".

Both The Mental Health Act and Regulation 729 specify that the request for information be in response to the written request of the administrator of a hospital or the chief executive officer of a health facility. As far as the legislation is concerned, the transfer of information does not occur as a matter of course. The practice, however, is quite different. Our examination of the policies, guidelines and by-laws of over 150 hospitals and psychiatric facilities in Ontario revealed that, when the transfer of a patient takes place, his or her health information is automatically forwarded to the facility to which he or she is being transferred without any written request or express patient authorization. A typical administrative policy of a public hospital governing the release of confidential patient information in cases of transfer reads as follows:

In the case of a transfer of a patient to any other hospital or health care facility, a copy of the pertinent parts of the chart should accompany the patient.

As this policy indicates, public hospitals do not confine their disclosure of a transferring patient's information to other hospitals as the Regulation contemplates; they also provide this information to other health care facilities. In their briefs, the Ontario Hospital Association, the University Teaching Hospitals Association, and the Ontario Medical Association submitted that this practice be legitimated by an appropriate amendment of the Regulation under The Public Hospitals Act to permit "the automatic provision of patient information at the time of transfer to certain other types of health care [facilities]", such as nursing homes, home care programmes, homes for the aged, or homes for special care, without a formal request or patient authorization. This submission merits consideration in view of my recommendation that all health-care facilities should be governed by the same or similar provisions for the protection

of the confidentiality of patient information. However, automatic release of confidential information offends the principle that patients have a right to control the communication of information about themselves, a right which is inherent in the concept of privacy I have endorsed for the purpose of this report. It should not be subordinated to institutional convenience unless it can be demonstrated that it is clearly in the best interests of patients to do so.

At our policy hearings, the Ontario Hospital Association was asked to explain the problems which requiring the patient's consent for transfer of information would present to hospitals. Mr. Roger Slute, executive director of Association Services, gave this reply:

May I lead off on that one, Mister President? Firstly there are two essential parts. One is the added paperwork where it really shouldn't be necessary in the hospital. Hospitals, as perhaps this Commission and perhaps my desk and others, is the inundation of paperwork should be fought wherever there is an alternative. Otherwise, you should buy stocks in all the paper companies. It is costly to produce extra pieces of paper, and goodness knows and so does everybody else that we are in a problem in this province in providing health care services because of the financial restraints. That's an added problem.

The other problem is that in particular The Homes for Special Care Act, there are a great many people I am led to believe in states of mental disability whose authorizations would not be valid, and those people who have been abandoned in fact by relatives and general people who could not consent for them.

It would be a very cumbersome process and costly again to apply to the Official Guardian for his consent, or someone else who can consent for that patient who doesn't have the status of next of kin. So what we are saying is that it would be most simple and most economical, because it is always in the patient's interest, that at least the discharge summary, if that's a proper piece

of paper in most hospitals' records, where the course of the hospital treatment, the diagnoses and the prognosis for the patient is put down, and that that should automatically go into these four cases where those organizations, the nursing homes, the homes for the aged and so on, do have their responsibilities assigned by law about confidentiality, and each kind, each one of those kinds is licensed or registered or recognized by a schedule under those Acts, by the government, as having rights and responsibilities and duties to their patients.

So if we could put it in, it would be certainly a valuable thing and a much more simple way of doing it. And we don't know of any case where a person would object. We have never heard of any. [emphasis added]

Although Mr. Slute said that he did not "know of any case where a person would object", the fact is that few patients are in a position to object, since hospitals neither allow patients to see their records to know what information is being transferred, nor give them any opportunity to object. That the automatic release of such information as the patient's discharge summary in cases of transfer is "always in the patient's interest" is not self evident. We have seen enough examples of the communication of inaccurate information, bringing about undesirable consequences, to cause one to hesitate to accept the assertion as universally valid. Moreover, to some patients the mere absence of consultation is objectionable. The 1978 Report of the Ontario Council of Health on Medical Record Keeping also questions the assumption that unauthorized transmittal is always in the best interest of the patient. At page 22 of that report the following statement is made:

Current legislation (Regulation 729, Section 48(5), under The Public Hospitals Act) permits the administrator of a hospital to transmit information and copies from the medical record upon the written request by the administrator of another hospital. It appears that there has been an assumption that such transfer of information between institutions is in the patient's best interest and therefore does not require his signed authorization. The Task Force,

however, believes that there should be transfer of information from one hospital administrator to another administrator only when the patient (or his next of kin or guardian) has given his written permission, and upon the submission of the administrator requesting information that he has written permission from the patient in his hospital to obtain such information, or that an emergency situation has occurred in which consent could not be obtained. The patient's written consent or a statement that consent could not be obtained because of the patient's disability must be transmitted to the administrator releasing the information as soon as possible.

The Council's recommendation for change in the legislation to make a patient's authorization mandatory in such situations would protect the patient's right to privacy, but, at the same time, it would erect an obstacle to the hospital's flow of information to another health facility for the purpose of continuity of patient care which, in some cases, may be impracticable and contrary to the welfare of the patient.

The solution adopted in other provinces is worthy of note. In The Alberta Hospitals Act, R.S.A. 1970, chapter 174, the provision of confidential information by the hospital transferring a patient without his authorization is not only permitted but is compulsory. Section 35(5.1) says:

The board of an approved hospital shall, after the discharge of a patient from the hospital for the purpose of transferring him to another hospital or nursing home inside or outside Alberta, forward to that other hospital or nursing home copies of the appropriate records of diagnostic and treatment services provided in respect of that patient for the use of the staff of that other hospital or nursing home.

This obligation is also present in a regulation pursuant to the Quebec Health Services and Social Services Act, 1971, S.Q. 1971, chapter 48. Section 3.5.6 of Regulation 3322-72 provides that:

Where a person is transferred from one establishment to another, the establishment where he was first admitted or registered



shall forward to the second a record summary within 72 hours.

Jean-Guy Fréchette, the author of an authoritative guide to the Quebec legislation, Access to Medical Record Information, has this to say about the time element:

Although the legislator has imposed a time limit, one must keep in mind, above all, that, in the case of a transfer, all information which is essential for the protection of the life of a patient or to ensure his physical well-being, must be transferred without delay, either by telephone or by another method of rapid communication. The delay of 72 hours mentioned in the law only applies to the report summary.

Clearly, Alberta and Quebec view the forwarding of patient information upon transfer as vital to the patient's health care.

As throughout this report, the challenge is to reconcile the competing interests involved, in this case, of institutional efficiency in treating patients, on the one hand, and confidentiality of health information, on the other. Neither interest can be said to be in the best interest of all patients in all circumstances. A compromise must be achieved. The solution proffered by the American Hospital Association in its publication, Hospital Medical Records, is that a patient, on admission to hospital, should be asked to sign a consent form allowing the hospital to transfer information to another hospital if the need should ever arise. Such a general and uninformed consent, signed before any information has ever been collected, and comprising part of the admission routine, is not, in my opinion, a satisfactory balancing of the conflicting interests. A preferable course is for the hospital, unless prevented by circumstances, to inform the patient, before any information is transferred, of the nature of the confidential information it plans to transfer with him or her to another health facility and the reason for the transfer, in order to enable the patient to express his or her disapproval of the disclosure, or any part of it, if he or she believes there is reason to do so. The qualification, "unless prevented by circumstances" makes allowance for those urgent situations in which time, or the patient's condition, does not permit the suggested procedure to be followed. After notification, the patient's wishes would be respected; the hospital must not be legally obligated to send the information regardless of the

patient's directions. However, it would not be necessary for the hospital to obtain a written consent from the patient in order to release the relevant information to the health facility to which he or she is being directly transferred. If the prevailing circumstances prevent the proposed procedure from being carried out this fact should be recorded and the patient should be informed as soon as possible thereafter. If, in the exceptional situation, a patient chooses to prohibit the disclosure of any or all of the information which the attending physician perceives to be imperative to his or her future health care, the prudent course for the physician to follow is to ask the patient to sign a statement to this effect.

*Recommendation:*

66. *That the legislation governing hospitals and health-care facilities permit the transfer of patient information to a designated receiver in another hospital or health-care facility to which a patient is being directly transferred without the written consent of the patient, provided that the patient (or the patient's representative) has been notified of the intended transmittal before it occurs in order that he or she may have the option to prohibit the disclosure. If the urgency of the situation or the patient's condition prevents this notification, this fact must be duly noted and the patient informed of the transfer of information as soon as possible after the fact.*

In his book, Access to Medical Record Information, Mr. Fréchette points out that sometimes even direct transfer is interrupted when there is a delay in the patient's entry into a long-term care centre, perhaps because of a shortage of beds; this should be treated as a direct transfer to permit the hospital to forward the information to the new health facility at a later date without the patient's written consent.

Another type of inter-hospital communication occurs when a patient, who has been treated by a hospital, is admitted to a second hospital at a later time, and the second hospital requests information about the patient's history and treatment from the first hospital. This situation is now controlled by the provisions of The Mental Health Act and Regulation 729 under The Public Hospitals Act discussed above, enabling the officer

in charge or the administrator of the second hospital to obtain the information on written request, without the authorization of the patient. In these circumstances, there is no reason why the patient, no longer under the care of the first hospital, should be denied the right to control this hospital's disclosure of his or her information. The second hospital is, in relation to the first, simply a third party, and ought not to be entitled to confidential patient information from the first hospital without the patient's consent under ordinary conditions. In cases of urgency the second hospital's oral representation that it has the patient's authority should suffice, provided the patient's written authorization is forwarded to the first hospital at the earliest opportunity.

As always, emergencies call for an exception to the general rule of patient authorization. In any situation in which the second hospital immediately needs confidential information about a patient because his or her life, health or safety is in jeopardy an unauthorized request from a second hospital should be honoured without delay. Regulation 729 under The Public Hospitals Act makes no allowance for emergency situations, but The Mental Health Act, section 26a(3)(e) permits the disclosure or the transmittal of the clinical record to "a person currently involved in the direct health care of a patient in a health facility" without the consent of the patient or nearest relative, "where delay in obtaining the consent of either of them would endanger the life, a limb, or a vital organ of the patient."

*Recommendation:*

67. *That, where the transfer of a patient is not involved, a hospital or health-care facility be permitted to release confidential patient information to another health facility without the consent of the patient if there is a threat to the patient's life, health or safety. In any other case the patient's authorization must first be obtained.*

Steps should, of course, be taken by the releasing hospital to assure itself that the request is indeed from another health facility and that it is not being made the victim of a pretext of the kind discussed at length elsewhere in this report. The procedures for verification and logging of emergency and non-emergency information requests should be contained in the hospital's information handling guidelines and by-laws as proposed earlier in this chapter.

## Disclosure by Hospitals to Physicians

Patients who are not transferred to another health-care facility are often encouraged to seek continuing medical attention from their own physicians or are referred to other health professionals for further care. Hospitals routinely send copies of the discharge summaries to their patients' family physicians, referring physicians or physicians to whom the patients are being referred upon discharge, without the consent of the patients. Although expressing the policy of one hospital responding to our survey, the following statement is typical of the practices pursued by public and psychiatric hospitals:

An authorization is Not required from a patient's family doctor or referring doctor.  
(Copies of Final Notes are routinely sent to these doctors and any further information requested can be sent out as well.)

I received submissions from individual patients complaining about the practice of non-consensual disclosure to physicians who referred the patients and physicians to whom the patients were referred. There are many reasons why a patient may not want his or her physician to be informed of his or her hospital treatment and diagnosis. Even more common among patients is the resentment that this disclosure occurs without their permission or even their knowledge. No support for this practice can be found in the legislation. Section 26a of The Mental Health Act does not permit disclosure to treating physicians other than those "employed in or on the staff of the psychiatric facility" or "currently involved in the direct health care of the patient in a health facility." Under section 48(5)(a) of Regulation 729 under The Public Hospitals Act, the hospital board "may permit...the attending physician...to inspect and receive information from a medical record and to be given copies therefrom"; the "attending physician" is defined in the Regulation as "a medical practitioner who attends a patient in the hospital."

The Ontario Hospital Association makes the following interpretation of this provision in its brief:

It is assumed, but it is not entirely clear, that in section 48(5)(a) of Regulation 729...the "attending physician" is the doctor who is actually looking after the health of a patient after discharge from hospital, regardless of whether or not the physician attended the patient in hospital or is a member of the hospital's medical staff.

The Association itself seems sceptical of the logic of this interpretation and sees a need for change or clarification of the authority of hospitals to release automatically confidential information to a patient's family physician or referring physician upon his or her discharge from hospital:

OHA recommends that the Commission propose such guidelines or changes to Regulation 729 as it considers necessary to provide that:

where the patient was referred to the hospital by a physician who is not on the medical staff, the hospital should be able to send to the physician a copy of the hospital discharge summary, report of treatment and diagnostic procedures, without the necessity of written authorization by the patient or his qualified representative;

This non-consensual disclosure by the hospital to an outside treating physician is similar to disclosure to another health-care establishment to which the patient is being transferred; both are considered by the Ontario Hospital Association to be "correct and desirable for the sake of the continuity of care of the patient and the avoidance of duplication of tests." This gives rise to the same problems encountered earlier, that of balancing a beneficial flow of information out of the hospital against the right of the individual to control the external circulation of his or her sensitive information. The patient's welfare should be the paramount concern in any reconciliation of the conflict and the patient's need for continuing and informed health care is an important factor in the reconciliation.

#### *Recommendation:*

68. *That the legislation permit hospitals and health-care facilities to transmit patient information, without the written consent of the patient, to the physician who referred the patient to the hospital or the physician to whom the patient is being referred by the attending physician for further care, provided that the patient (or the patient's representative) has been notified of the intended transmittal before it occurs in order that he or she may have the option to prohibit the disclosure. If the urgency of the situation or the patient's*



*condition prevents this notification, this fact must be duly noted and the patient informed of the disclosure of information as soon as possible after the fact.*

After the patient's discharge from the hospital, the situation also arises in which a new physician requests confidential information about his or her new patient from a hospital which the patient has attended. In these circumstances, the written authorization of the patient should be a prerequisite to the release of any information to the patient's new physician. I agree with the submission on this point of the Ontario Hospital Association:

OHA recommends that the Commission propose such guidelines or changes to Regulation 729 as it considers necessary to provide that:

*...where, after discharge from the hospital the patient chooses a family physician who is not on the hospital medical staff, and including cases where the patient moves out of Ontario, the hospital should send appropriate medical data to that physician only on the written authorization of the patient or his qualified representative.*

The requisite written authorization for hospital disclosure to a patient's physician may be forgone in the case of emergencies where the life, health or safety of the patient is immediately endangered. Reasonable efforts should be made to ensure that the request is genuinely that of the patient's physician before information is disclosed. Again, the hospital should develop procedures for releasing information under these emergency circumstances.

*Recommendation:*

- 69. That, where a referral by the attending physician to another physician is not involved, legislation permit a hospital or health-care facility to release confidential patient information to the patient's physician without the consent of the patient if there is a threat to his or her life, health, or safety. In any other case, the written*

*authorization of the patient must first be obtained.*

### Patient Inquiries

On the admission of a patient to a hospital as an in-patient, a number of departments are immediately notified and informed of his or her location in the hospital and general condition (when it becomes available) for the purpose of answering inquiries from the public. This routine hospital practice of divulging information to any inquirers, without the consent of the patient, is not recognized or authorized by the present legislation. However, it is probably the expectation of the patient, his or her relatives and friends and the public generally that this service will be provided by a hospital for the sake of convenience. It seems to be neither reasonable nor appropriate to expect the hospital to obtain every patient's formal consent before it may indicate to the general public whether a patient has been admitted to hospital and state, in the most general terms, how serious the patient's current condition is. This, however, is a practice which I believe a patient has a right to limit or forbid.

A patient's right to control the public dissemination of his or her admission and health status information is dealt with in section 123 of the U.S. Bill H.R. 5935, the "Federal Privacy of Medical Information Act". The proposal is as follows:

A medical care facility may disclose medical information it maintains about a patient, without the [patient's] authorization described in section 115(a), if the disclosure only reveals the presence of the patient at the facility, his location in the facility, and his general condition, and

- (1) the patient has not objected in writing to the disclosure, and
- (2) the information does not reveal specific information about the patient's condition or treatment.

A much broader provision for this type of disclosure is found in section 63(7) of The Public Hospitals Act of Nova Scotia, R.S.N.S. 1967, chapter 249, as amended by S.N.S. 1977, chapter 45:

Nothing contained herein prevents a hospital or a qualified medical practitioner from disclosing general information on the condition of a person or patient unless that person or patient directs otherwise.

Both the hospital's right to release this information and a patient's right to object should be set out in legislation. If a patient does not want the fact of his or her admission to hospital or his or her condition revealed, the patient should be entitled to sign a simple statement to this effect.

#### *Recommendation:*

70. *That legislation permit a hospital or health-care facility to reveal the presence of a patient, his or her location and his or her general condition to any person who inquires, but only if the patient (or the patient's representative) has not objected, in writing, to this disclosure. The hospital or health-care facility shall not reveal specific information about the patient's condition or treatment unless required or permitted by law.*

#### The Press

The question of access by the press to hospital patient information is a difficult one. I include the electronic media in the term, the press. At the present time, most hospitals in Ontario follow the Ontario Hospital Association's Recommended Press Code either in whole or in part, a code developed in 1966 to ameliorate what the Association called "a general climate of uncertainty and even antagonism between hospitals and media people, with hospital staff on the one hand refusing to provide any information whatsoever and news reporters, in retaliation, adopting questionable practices and subterfuges to ferret out the information they sought." The purpose of the code was to encourage consistent procedures among hospitals in their response to press inquiries, and, at the same time, to limit the amount of information released.

The code draws a fundamental distinction between the release of information concerning a patient whose case could be described as being on the "public record", that is, one reported to such public authorities as the police and fire departments,

and a patient whose case is not one of public record. According to the Recommended Press Code, provided that the patient's next-of-kin has been notified, the patient's consent is not required for the hospital to release the following information in "cases of public record":

Name  
Married or Single  
Address  
Sex  
Age  
Occupation  
Time of arrival

General condition - good, fair, serious,  
critical

Nature of accident - (without cause)

Attending Physician - (with physician's  
consent)

Nature of injuries or illness

However, if the case is one of sexual assault, suspected drug addiction, abortion, or a psychiatric or maternity emergency, it recommends that the hospital release the patient's condition only, with no identifying information to the press.

At the present time there is no legislative provision authorizing the release of any confidential information to the press, whether it be in accordance with the Recommended Press Code or not. In its brief the Ontario Hospital Association submitted that the "present legislation be adjusted to legitimize the present situation", and "that the OHA's Recommended Press Code be recognized by the Commission as an acceptable guide for the purpose." It is my opinion, however, that the press, whose function it is to inform the public, has no higher "right to know" confidential health information than the public generally. Its access should be limited to patient health information that anyone making a general inquiry about an in-patient could receive from the hospital without the consent of the patient, that is, the fact of the patient's presence, his or her location and general condition. That the patient has been unfortunate enough to be injured in such a way that the incident is of public record is not a justification for the particulars of his or her injuries or illness being made public knowledge without his or her consent.

## Police

Generally speaking, hospitals and health-care facilities have no authority to disclose information to a police officer except pursuant to legal process or with the patient's written consent. However, our investigation revealed that in the past, hospitals have disclosed confidential patient information to the police without authorization, despite the existing legislation. Some hospitals have contacted the police when they treated patients with gunshot or stab wounds consistent with violent or criminal activity. When police make inquiries concerning a suspect who is known to have suffered a specific type of injury, hospitals often disclose relevant information. These hospitals feel that it is their social duty to aid the police with respect to law enforcement and national security, even though this duty conflicts with another which is also in the public interest, namely, their responsibility to protect the privacy of their patients' sensitive information. These competing interests must be balanced and the rights and responsibilities of the police and patient must be clarified in the legislation. Elsewhere in this report I discuss the relationship between patient confidentiality and the legitimate needs of law enforcement, and make recommendations which apply to hospitals and health-care facilities.

## Correctional Institutions

When a person, who is confined to a correctional institution within the meaning of The Ministry of Correctional Services Act, 1978, S.O. 1978, chapter 37, requires medical treatment from a public hospital or a psychiatric facility, he or she must be referred to such an institution pursuant to section 24 of that Act:

(1) Where a person confined in a correctional institution requires hospital treatment that cannot be supplied at the institution, the director or superintendent shall arrange for the person to receive such treatment at a public hospital and shall report the matter to such persons as the Minister may require.

(2) Where a person confined in a correctional institution requires hospitalization in a psychiatric facility under The Mental Health Act, the director or superintendent shall arrange for the person to be so



hospitalized and shall report the matter to such persons as the Minister may require.

. . . . .

(4) The Minister may, by order, direct that an examination be made of an inmate by a psychiatrist or psychologist in a manner prescribed by the regulations for the purpose of assessing the emotional and mental condition of the inmate.

The superintendent or medical officer of the correctional institution may need to acquire medical information about the patient from the treating health-care facility in order that any special diet, drugs or care may be provided for on the patient's return to the correctional institution. However, neither Regulation 729 under The Public Hospitals Act nor The Mental Health Act permits such a disclosure.

The problem can be avoided, of course, if the patient signs a form authorizing the release of his or her confidential medical information from the hospital or psychiatric facility to a representative of the correctional institution, but a patient in custody may be unwilling to sign a consent form. Without the patient's consent, the hospital or psychiatric facility has no authority to co-operate with the custodial institution to protect the health of the inmate. The U.S. Bill H.R. 5935, the "Federal Privacy of Medical Information Act", contains the following proposal for disclosure to a patient's custodian:

Sec. 130(a) A medical care facility may disclose medical information it maintains about a patient, without the authorization described in section 115(a), if the disclosure is

. . . . .

(2) to the custodian of the patient, if the patient is an inmate or resident of a penal, correctional, detention, or other similar custodial facility and the information relates to the current treatment of the patient and is reasonably necessary in order to protect the health of the patient.

The Ontario Hospital Association requested that the position of the hospital with respect to disclosure to a correctional institution be clarified and suggested,

...that the Commission issue guidelines or recommend changes in the legislation which will permit hospitals to provide copies of medical records or parts thereof...to the medical officer of a correctional institution...without the necessity of patient authorization.

*Recommendation:*

71. *That legislation governing confidential information maintained by hospitals and health-care facilities permit the disclosure of information concerning a patient who is confined in a correctional institution and who has been hospitalized, to the superintendent, director or medical officer of the patient's institution, for the purpose of maintaining the health of the patient, provided that the patient is notified of the disclosure.*

Research

As I have already pointed out, the officer in charge of a psychiatric facility "may disclose or transmit the clinical record to or permit the examination of the clinical record by...a person for the purpose of research, academic pursuits or the compilation of statistical data" under section 26a(3)(f) of The Mental Health Act. However, it is only "a member of the medical staff" in a public hospital, who may be permitted "to inspect and receive information from a medical record" under section 48(5)(d) of Regulation 729 under The Public Hospitals Act and only then for teaching purposes or for a scientific research project which has been "approved by the medical-staff advisory committee." Several submissions expressed concern over the failure of the legislation governing public hospitals to permit the disclosure of information to researchers who were not members of the hospital's own medical staff. E.R. Willcocks, the executive director of the Toronto East General and Orthopaedic Hospital, Inc. made the point in this way:

There is nothing in the Public Hospitals Act that relates directly or permits this...but hardly a week goes by, and now I am speaking of our own situation at Toronto East General Hospital, where we do not receive a request from a Resident or Fellow in another hospital for information concerning a group of patients with a specific diagnosis in the name of research.

The Brantford General Hospital expressed the problem in the following language:

Recently we have been in receipt of a letter from a Medical Education Department of a large University, requesting that we co-operate with their faculty of Health Sciences, participating in a study in co-operation with the College of Family Physicians of Canada. This would require the records of all patients treated in this hospital by two of our staff doctors, between April 1976 and October 1977. The records would be reviewed by trained and experienced nurse abstractors. We realize it is very unlikely that any confidential information in this study would ever leak to outside persons. However, it is a third party examining the confidential medical records of a patient without that patient's knowledge. We are in receipt of signed consents by both of the doctors involved.

There is a portion of the Public Hospitals Act allowing a member of the medical staff access to medical documents of other patients for teaching purposes or scientific research, but it would not cover situations such as I have just described. I think this is one area where perhaps some change in legislation should be made to allow teaching centres to carry on such studies as they certainly are in the interest of the patient.

Some public hospitals treat requests for confidential patient information for research purposes from persons outside the hospital in the same way as internal requests, that is, by presenting them to the medical advisory committee for approval.

It is apparent that Regulation 729 did not anticipate the significant role hospital records play in clinical and epidemiological research projects which, in turn, benefit the health and well-being of the public at large.

In its brief, the Ontario Hospital Association made the following submission:

OHA recommends that the Commission issue such guidelines as it considers desirable to assist researchers and hospitals to understand the methodology to be followed in obtaining confidential information.

Elsewhere in this report the subject of research and the problems of researchers are discussed. The recommendations made there are intended to provide a practical procedure to facilitate health research using confidential patient information and, at the same time, protect as much as possible the privacy of patients.

### The Coroner

According to section 13(1) of The Coroners Act, 1972, S.O. 1972, chapter 98, the coroner must investigate the death of any person in the province whose death is reported to have occurred under any of the circumstances set out in section 9 of the Act, as amended by S.O. 1978, chapter 38, sections 4(2), (3). These circumstances include death while a resident, in-patient or inmate of certain health-care institutions, including, in some instances, hospitals. Under The Coroners Act, 1972, as amended by S.O. 1974, chapter 103, section 6, the coroner's powers while investigating a death include the right of access to any relevant information about the deceased:

13. (1) Where a coroner is informed that there is in his jurisdiction the body of a person and that there is reason to believe that the person died in any of the circumstances mentioned in section 9, he shall issue his warrant to take possession of the body and shall view the body and make such further investigation as is required to enable him to determine whether or not an inquest is necessary.

. . . . .

14. (2) A coroner may, where he believes on reasonable and probable grounds that to do so is necessary for the purposes of the investigation,

- (a) inspect any place in which the deceased person was, or in which the coroner has reasonable grounds to believe the deceased person was, prior to his death;
- (b) inspect and extract information from any records or writings relating to the deceased or his circumstances and reproduce such copies therefrom as the coroner believes necessary;
- (c) seize anything that the coroner has reasonable grounds to believe is material to the purposes of the investigation.

. . . . .

(4) A coroner may, where in his opinion it is necessary for the purposes of the investigation, authorize a legally qualified medical practitioner or a police officer to exercise all or any of his powers under clauses a, b, and c of subsection 2 but, where such power is conditional on the belief of the coroner, the requisite belief shall be that of the coroner personally.

(5) Where a coroner seizes anything under clause c of subsection 2, he shall place it in the custody of a police officer for safe keeping and shall return it to the person from whom it was seized as soon as is practicable after the conclusion of the investigation or, where there is an inquest, of the inquest, unless he is authorized or required by law to dispose of it otherwise.

. . . . .

This right of access includes any information about the deceased maintained in a hospital or other health-care facility. Section 48 of Regulation 729 under The Public Hospitals Act contains a



compatible clause, allowing public hospitals to release information from medical records to coroners or their authorized representatives:

48. (1) Subject to subsections 2, 3, 4 and 5, a board shall not permit any person to remove, inspect or receive information from a medical record.

. . . . .

(3) Notwithstanding subsection 1, a coroner or a legally qualified medical practitioner, magistrate or police officer so authorized in writing and directed by a coroner, may inspect and receive information from medical records and may reproduce and retain copies therefrom for the purposes of an inquest or to determine whether an inquest is necessary, where the coroner has,

- (a) issued his warrant to take possession of the body;
- (b) issued his warrant for an inquest;  
or
- (c) attended at the hospital to view the body and make an investigation in accordance with The Coroners Act.

In his brief, Dr. H.B. Cotnam, the Chief Coroner for Ontario, made note of the contrast between the language of section 48(3), in which access to "information from medical records" is permitted, and section 14 of The Coroners Act, 1972 quoted earlier, allowing access to "information from any records or writings relating to the deceased." According to Dr. Cotnam, this latter section "includes not only hospital medical records, but medical records in any other places such as in the offices of the attending physician or consultants." Earlier, I discussed the presence in hospitals of confidential information which is not a part of the official medical record as defined by Regulation 729. I agree with Dr. Cotnam that The Coroners Act, 1972 allows access to more than medical record information. Dr. Cotnam's proposal to resolve this inconsistency was the following:

In view of the fact that there is a conflict between Section 14(2)(b) of The Coroners

Act, and Regulation 729, Section 48(3) of The Public Hospitals Act, we would recommend that subsection (3) be revoked.

Revoking the provision specifically authorizing public hospitals to release this medical record information to coroners would leave these hospitals in uncertainty as to the authority of coroners to have access to the patient information in their hospital. Instead, it would be preferable that the legislation governing hospitals and the inspection and receipt of their patient information by a coroner be made consistent with the provisions in The Coroners Act, 1972.

Section 26a of The Mental Health Act does not mention the disclosure of patient information in a psychiatric facility to a coroner. This lack of specific authority for a coroner's access appears to place The Mental Health Act in conflict with the coroner's right of access under The Coroners Act, 1972, since section 3 of The Mental Health Act states that:

...where the provisions of any Act conflict with the provisions of this Act or the regulations, the provisions of this Act and the regulations prevail.

The Ontario Hospital Association suggested that "the powers conferred upon a coroner by The Coroners Act...may be null and void" in psychiatric facilities. It is possible that subsection 5 of section 26a of The Mental Health Act could be interpreted as authorizing a psychiatric facility to release information to the coroner:

Subject to subsection 6 and 7, the officer in charge or a person designated in writing by the officer in charge shall disclose, transmit or permit the examination of a clinical record pursuant to a subpoena, order, direction, notice or similar requirement in respect of a matter in issue or that may be in issue in a court of competent jurisdiction or under any Act.

In the view of the Ontario Hospital Association, this subsection is "confusing to many who are governed by this Act. It is not known what a 'direction, notice, or similar requirement' might be." I agree. There should be no confusion. Legislation governing all types of health facilities with respect to the examination and receipt of information by coroners should be

clarified and made consistent with the powers of investigation given to coroners under The Coroners Act, 1972.

*Recommendation:*

72. *That legislation governing the confidential patient information in hospitals and health-care facilities authorize the examination and receipt of any patient information by a coroner or his authorized representatives in accordance with the provisions of The Coroners Act, 1972.*

Another inconsistency between The Coroners Act, 1972 and Regulation 729 under The Public Hospitals Act with respect to the release of confidential patient information was the subject of comment by Dr. Cotnam, the Ontario Association of Pathologists, and the Ontario Hospital Association. It concerns the release of patient information from a coroner to a hospital. According to section 23 of The Coroners Act, 1972, as amended by S.O. 1978, chapter 38, section 13, a coroner may issue his warrant for a post mortem examination of a body and distribute the result of the findings, that is, the medico-legal post mortem examination report, to designated recipients. Section 23 reads as follows:

(1) A coroner may at any time during an investigation or inquest issue his warrant for a post mortem examination of the body, an analysis of the blood, urine, or contents of the stomach and intestines, or such other examination or analysis as the circumstances warrant.

(2) The person who performs the post mortem examination shall forthwith report his findings in writing only to the coroner who issued the warrant, the Crown attorney, the regional coroner and the Chief Coroner, and the person who performs any other examination or analysis shall forthwith report his findings in writing only to the coroner who issued the warrant, the person who performed the post mortem examination, the Crown attorney, the regional coroner and the Chief Coroner.

If the body being examined is that of a patient who has died in a hospital, the intent of Regulation 729 is not fully met. Section 23(2) does not allow the coroner to provide the hospital with a report of the post mortem examination for its medical records. Regulation 729 under The Public Hospitals Act contains these provisions:

38. (1) The board shall cause to be compiled for each patient a medical record including,

. . . . .

(h) reports of,

. . . . .

(ix) post mortem examination, if any;

. . . . .

41. When a medical practitioner performs a post mortem examination on the body of a patient, he shall make and sign a report of the examination and deliver it to the superintendent.

Until mid-1977 hospitals were provided with a copy of this report by the coroner when the investigation or inquest proceedings were concluded, despite section 23(2) of The Coroners Act, 1972. That practice has since stopped. In June, 1977, Dr. Cotnam sent a memorandum to all coroners and regional pathologists in Ontario containing guidelines for the disposition of medico-legal post mortem examination reports, and prohibiting their inclusion in the medical record of a hospital:

Medico-legal autopsy reports are Crown documents. The original report and notes shall be kept in the custody of the person who performed the autopsy, and not in the general Medical Records Department of the hospital, nor shall a copy be included in the Medical Records.

In his presentation at our hearings, Dr. Michael Dietrich, past president of the Ontario Association of Pathologists, discussed the exclusion of these reports from the hospital medical record, and described the importance that post mortem

examinations made under The Coroners Act, 1972 can have. They give immediate information to the attending physician of the deceased patient, and educate other physicians on the staff of the hospital, who discuss the findings of the post mortem examination at their medical staff meetings. The Ontario Hospital Association also reported that a number of its member hospitals had protested about the absence of these reports in their hospitals for education and quality control purposes. In his memorandum, Dr. Cotnam recognized the value of the reports to the attending physicians:

Inasmuch as the attending physician is required to give information on the case to the coroner and/or the pathologist prior to or during the autopsy, he is entitled to receive a verbal report on the findings, except on cases included in Category B. above.

He may receive a copy of the official autopsy report with the permission in writing of the next-of-kin as identified in section 16(2) of The Coroners Act, or he may request a copy through my office.

The investigating coroner may authorize the autopsy findings, and other relevant reports, to be discussed at Medical Staff Meetings, on cases where death occurred in their respective hospitals.

The time of release of the autopsy report will be determined by the coroner in each case. No report shall be released until the coroner has determined that the investigation and/or inquest has been terminated, nor shall it be released under any circumstances if police investigation is continuing in cases of homicide, foul play, etc. Cases falling into this latter category should never be released, but it is my understanding that these are not the cases which need to be reviewed by Death Committees of hospitals.

This state of affairs is criticized by the Ontario Association of Pathologists. As its president, Dr. Hugh Van Patter, explained at one of our policy hearings,



...the essence of it is that we feel that the medico-legal autopsy reports on patients who have been hospitalized and have gone into hospital should be incorporated in the medical charts of those hospitals after due consideration by the coroner and his agreement that there is no further purpose of not doing so, rather than having them kept only in the Chief Coroner's office available only verbally to the hospital. We feel that for purposes of medical education and the information of attending physicians it is important that those reports be in the hospital chart and that they can be referred to there in analysis of cases over the years to come, as well as giving immediate information to the attending physician. That's simply our point.

At the same hearing I asked Dr. Ross C. Bennett, Deputy Chief Coroner for Ontario, the reason for preventing the autopsy report of the pathologist from becoming part of the chart. The following discussion resulted:

DR. BENNETT: Well, speaking for the Chief Coroner, we have some reservations about making this a general policy to let the medico-legal post mortem report go to the hospital records sort of without some discretion given to the Chief Coroner. The reason is that it's a little different... it's a separate type of examination for a different purpose really. We would like to retain some control over these reports in spite of the fact that some cases are closed fairly shortly after the results are available. But the Chief Coroner prefers to be able to direct them to the appropriate sources who require them, at his discretion. That's the reason for this policy.

. . . . .

The information is available. The policy that has been put out by the Chief Coroner allows that report to be utilized by the medical staff for medical grounds, for discussions by the medical guidance committee, whatever the grounds requiring it.

MR. COMMISSIONER: If that's the case, what harm is there in allowing the copy to reside in the file?

DR. BENNETT: Well now that the medical records are a little more secure than they were formerly, I don't think we are against it, but the way it was prior to this Commission there was a concern that putting them on the records in certain hospitals would make them very available to any, to many eyes.

MR. COMMISSIONER: Can I exclude this possible explanation? Is it a concern that some of these cases will result in criminal charges being laid, and it is thought to be less than desirable that, let us say the person charged with the offence, or his counsel, should have access to the report of the pathologist until such time as the Crown decides to make it available at trial? Is that a possible reason?

DR. BENNETT: That is one of the reasons, and a small number of the reports would be handled in that manner.

MR. COMMISSIONER: But is that a valid reason? Is there any reason why a person charged with, let's say, a homicide should be prevented from having access to the report which sets out the cause of death? I would have thought the argument would be the other way, that if the cause of death indicates something other than the act of the person charged with the offence, the interests of justice require it be known to the accused as soon as possible.

DR. BENNETT: I would say that the information is available for the defence as well as the Crown, as well as the attending physician, the way the present system is.

MR. COMMISSIONER: Then if that is the case, what prejudice occurs to anybody by allowing, in the fullness of time, a copy of that report to be put in the patient's chart?

DR. BENNETT: I am not arguing against this. I agree with your statement. I said a policy has been developed according to the present Act, and if it was changed we would certainly go along with any suggestion you have.

MR. COMMISSIONER: Well, what I'm asking is, are there sound policy reasons for doing otherwise than recommending a change in this direction?

DR. BENNETT: Not that I am aware of.

Although I am sympathetic to the submission that the medico-legal post mortem examination report be incorporated into the medical record, I refrain from making a recommendation to this effect because I regard the question of what the medical record ought to consist of to be beyond my terms of reference.

### Reporting Requirements

Various Ontario statutes and regulations place a duty on hospital officials and other institutional health-care providers to report confidential information about certain of their patients to specified outside authorities, without the consent of the patients concerned. Two kinds of mandatory reporting provisions are relevant in this context: reporting which must be initiated by the health-care provider and reporting which must be made in response to a request.

The first type of reporting provision imposes a duty upon a hospital official or health-care provider to initiate a report when he or she becomes aware of the existence of a communicable disease, for example, venereal disease, or a condition or disease which, though not communicable, may nevertheless affect the health and safety of the subject or other persons. An example of the latter category is found in section 49(2) of The Child Welfare Act, 1978, S.O. 1978, chapter 85, whereby a health-care professional must report to a children's aid society if he or she suspects that a child "has suffered or is suffering from abuse that may have been caused or permitted by a person who has or has had charge of the child...". Further examples of this type of requirement are discussed in the section of this report on the mandatory reporting of health information, and the relevant Acts and regulations are listed in an appendix thereto.

Although these provisions oblige health-care institutions to report certain patient-identifiable health information to third parties, the legislation directly governing the release of information from a public hospital medical record, or from the clinical record of a psychiatric facility does not authorize disclosure in any of these cases. Requiring these disclosures without the consent of patients makes a public hospital, in the words of the Ontario Hospital Association, "by-pass the prohibition established in section 48 of Regulation 729 under The Public Hospitals Act about the release of information." In the case of section 26a of The Mental Health Act, the inconsistency between its disclosure proscription and the statutory reporting requirements of other legislation is even more marked, as section 3 of the Act says that the provisions of The Mental Health Act prevail over conflicting provisions of any other Act. According to the Ontario Hospital Association one of the practical results of this legislative confusion involving the release of information from psychiatric units of public hospitals is that "designated communicable diseases might not be reported."

An example of the second type of reporting provision, namely one which requires reporting upon request, is found in section 52 of The Workmen's Compensation Act. Section 52 reads as follows:

Every physician, surgeon, hospital official or other person attending, consulted respecting, or having the care of, any employee shall furnish to the Board from time to time, without additional charge, such reports as may be required by the Board in respect of such employee.

However, the legislation governing the release of confidential patient information from hospitals and health-care institutions does not authorize disclosure of patient information to the Workmen's Compensation Board. As a result, health-care facilities are not sure whether they are, indeed, required to make the disclosure. Our review of the policies and procedures of hospitals throughout the province revealed a great deal of confusion and inconsistency. This is not the case in such other jurisdictions as Alberta, where the legislation governing hospitals and mental facilities includes authority to release confidential information to the Workmen's Compensation Board, in accordance with The Workers' Compensation Act, 1973, S.A. 1973, chapter 87.

Ontario statutory reporting requirements placing a duty on hospitals and other health-care providers to supply medical reports to various public health and social service agencies, as well as at the request of the Workmen's Compensation Board, reflect policy decisions of the Legislature to prefer the benefits to society which reporting is thought to bring about over the right of privacy in those specified circumstances. Whenever mandatory reporting is prescribed, there should be a corresponding concern to ensure that the patients affected are provided with a legitimate "expectation of confidentiality" by clearly defining the limits of non-consensual disclosure in the legislation governing the confidential information maintained by hospitals and other health-care facilities.

#### *Recommendation:*

73. *That the reporting of confidential information to designated authorities under mandatory reporting requirements be reflected in legislation governing the confidentiality of patient information maintained by hospitals and health-care facilities by identifying every reporting requirement.*

#### Professional Colleges

The College of Physicians and Surgeons of Ontario is a statutory body responsible for licensing physicians to practise in Ontario, ensuring that its members maintain a certain standard of excellence in their practice of medicine, and disciplining members found to be guilty of either misconduct or incompetence. The objects of the College are set out in section 46(2) of The Health Disciplines Act, 1974, S.O. 1974, chapter 47. Under section 64 of the Act, a person appointed by the College to make an investigation to ascertain whether an act of professional misconduct or incompetence has occurred may examine the practice of the member, and may, "upon production of his appointment, enter at any reasonable time the business premises of such person and examine books, records, documents and things relevant to the subject-matter of the investigation", with the powers of a commission under Part II of The Public Inquiries Act, 1971. Under sections 48(4) and (4a) of Regulation 729 (as amended by O. Reg. 193/72, section 1) under The Public Hospitals Act, the College is given the following right of access to public hospital medical records:



48. (1) Subject to subsection 2, 3, 4 and 5, a board shall not permit any person to remove, inspect or receive information from a medical record.

. . . . .

(4) Notwithstanding subsection 1,

(a) the registrar and the elected members of the Council of The College of Physicians and Surgeons of Ontario, ex officio; and

(b) a medical practitioner or medical practitioners appointed by The College of Physicians and Surgeons of Ontario,

after giving notice to the administrator may, for the purposes of the College,

(c) inspect and receive information from medical records and may reproduce and retain copies therefrom; and

(d) require all members of the medical staff and hospital employees to answer inquiries concerning the admission, treatment, care, conduct, control and discharge of patients or any class of patients and the general management of the hospital insofar as that relates to the hospitalization of the particular patient or patients whose care and treatment are being investigated by the College.

(4a) The registrar of The College of Physicians and Surgeons of Ontario shall make a full and complete report in writing to the Minister forthwith after receiving

any report made to the College under sub-section 4.

The College of Physicians and Surgeons of Ontario, is, of course, only one of the five professional colleges governed by The Health Disciplines Act, 1974, the other disciplines being dentistry, nursing, optometry and pharmacy. The same investigative powers given to The College of Physicians and Surgeons of Ontario in section 64 of the Act are also given to the Royal College of Dental Surgeons of Ontario in section 40, to the College of Optometrists of Ontario in section 110, and to the Ontario College of Pharmacists in section 136 of The Health Disciplines Act, 1974. The College of Nurses of Ontario is the only college without these investigatory powers, perhaps because nurses are not thought to have a "practice" with "business premises." During our inquiry it was pointed out that professional colleges other than The College of Physicians and Surgeons of Ontario, and in particular the College of Nurses of Ontario, at times require access to confidential information maintained by hospitals and other health-care facilities in the course of investigating the care provided by their members, although this access is not permitted under the present legislation. The College of Nurses of Ontario, for example, receives complaints about the practices of the registrants of its College from employers (such as hospitals), other registrants, or from members of the public. I was told by this College that until 1978 it had little problem in gaining access to hospital medical records in order to investigate the conduct or competence of a registrant and to fulfil its peer review and disciplinary functions set out in The Health Disciplines Act, 1974. Hospitals have recently become more and more unwilling to open their medical records to investigative officers from the College of Nurses of Ontario, a trend the College attributes largely to increasing public sensitivity to the confidentiality of the records.

At the present time, the College of Nurses of Ontario must rely on the only available statutory method of obtaining access to patient records, the summons authorized by The Statutory Powers Procedure Act, 1971, S.O. 1971, Vol. 2, chapter 47. The College complains that under this procedure the records are not obtained until the date of the hearing so that as soon as the hearing is convened it has to be adjourned to permit both the College and defence counsel an opportunity to examine the records. The College's brief puts the matter this way:

Lack of authorized access to records in advance of a hearing necessitates review by both parties of larger portions of the health records than might be necessary if

investigators had had time to be selective. Thus unnecessary detail may be divulged. As well, time and money is wasted through adjournments, and calling of more evidence and witnesses by the defense, which might not have been necessary if there had been time for appropriate study.

Elsewhere, the submission says:

Authorized access to health records similar to that granted to the College of Physicians and Surgeons of Ontario under Regulation 729, Section 48(4) under the Public Hospitals Act, is essential for our investigators if they are to continue to carry out their function effectively. Administrators of health service agencies and institutions require specificity in regulations to protect themselves from charges of breach of confidentiality. We believe there should be such a regulation under the following acts: Public Hospitals Act; Nursing Homes Act; Public Health Act; Mental Hospitals Act; and Occupational Health Act.

The Ontario Hospital Association supports the College of Nurses of Ontario on this issue, adding that "certainly at times the procedures adopted by that College to obtain evidence cause problems for hospitals" as well as the College. The Association's brief continues:

An example is the issuance of a summons requiring a witness to appear at a College [of Nurses] hearing and bring "all of the documents and records specified" in an accompanying schedule. The document sent to the hospital was not signed by any person and a copy is attached as Exhibit A.

As many as 18 medical records have had to be copied by a hospital for the purposes of a single investigation by the College and as many as 15 members of one hospital's nursing staff were required to travel to Toronto to appear as witnesses at a College hearing. Such demands create considerable expense and scheduling difficulty for the hospitals and a better solution should be found to this

aspect of self-government by the independent professions.

One recourse is to permit each College, prior to a formal hearing, to examine the medical records which were pertinent to the case. The Ontario Hospital Association has proposed to the Ministry of Health that a new subsection, as recommended below, be added to section 48 of Regulation 729. This would not limit the special authority and access already provided to the College of Physicians and Surgeons of Ontario.

#### Recommendation 4

OHA recommends that section 48 of Regulation 729 be amended by adding a new subsection 4b as follows:

48(4b) Notwithstanding subsection 1, the Registrar and the elected members of the council of a college established by the Health Disciplines Act, 1974 ex-officio, and a practitioner member of a college appointed by the council of the college, after giving notice to the administrator, for the purpose of the respective college investigating one of its members, may inspect and receive information from a medical record and may reproduce and retain copies therefrom.

During our policy hearings, R. Alan Hay, executive director of the Ontario Hospital Association made the following distinction between his Association's recommended access by the "other" colleges and that of The College of Physicians and Surgeons:

Well we make a differentiation between The College of Physicians and Surgeons' special requirements and the requirements that we see other colleges under the Health Disciplines Act have. This is the important... but we don't think the other colleges should have access to whole records. They are really, in the case of the nurses, they want access to those parts of the record, nurses' notes or, that will help the College of Nurses ascertain whether the girl is competent or acting improperly or incompetently

or whatever. That's why we make this differentiation.

The 1978 Report of the Ontario Council of Health on Medical Record Keeping supports the expansion of the present hospital release provisions to include access by the College of Nurses of Ontario and the Royal College of Dental Surgeons of Ontario.

All of the Colleges included in The Health Disciplines Act, 1974 are bodies which are legally responsible for the conduct, continuing competence, and discipline of their members. All but the College of Nurses of Ontario already have extensive powers of investigation of confidential patient documents with respect to "the business premises" of their members, in order to discharge these responsibilities. In the case of medical records in hospitals and other institutional health-care providers, access should be provided to information about the care and treatment of a patient by the college member being investigated. There has been no challenge to the legitimacy or appropriateness of access by The College of Physicians and Surgeons of Ontario to confidential patient information from hospitals and health-care facilities, without the patient's consent, in order to meet its responsibilities and to protect the public from improperly conducted medical practices. The other colleges, whose members practise in hospitals and whose functions are equally significant to the quality of health care received by the public, should have the same right of access.

#### *Recommendation:*

74. *That legislation governing hospitals and health-care facilities permit the appropriate representative appointed by any college governed by The Health Disciplines Act, 1974 the same right to examine and receive confidential patient information as is now found in section 48(4) of Regulation 729 with respect to The College of Physicians and Surgeons of Ontario.*

#### Government Recipients

Patient health information and other patient information held by institutional health-care providers are collected, inspected and audited by a variety of provincial government departments and offices for various purposes often not clearly defined with relation to the information being inspected or



obtained. Information from patients' files is used by the government in connection with the health insurance plan, programme evaluation and management of health-care costs, overseeing the delivery of health-care services, planning modifications in facilities and services, and monitoring compliance with governing laws and regulations. The present practices of government in examining and collecting patient-identifiable information maintained by health-care institutions and the legislation regulating these practices have raised questions about patient privacy.

Because of its role in funding health-care facilities, the Ministry of Health receives information about insured services or other treatment obtained by patients in a hospital or health-care facility. Sections 57 and 58 of Ontario Regulation 323/72 under The Health Insurance Act, 1972, S.O. 1972, chapter 91, read as follows:

57. Every hospital in Ontario designated for the purpose of the Plan shall forward to the General Manager,

- (a) within twenty-four hours after an in-patient is admitted, a notification of admission in the prescribed form and if ambulance service has been required, a notification of the name of the ambulance operator listed in Schedule 11 who provided such service, together with the amount of ambulance service charges;
- (b) within ninety-six hours after an in-patient is discharged from or dies in the hospital, a notification of the discharge or death in the prescribed form and if ambulance service was required when the patient was discharged, a notification of the name of the ambulance operator listed in Schedule 11 who provided such service, together with the amount of the ambulance service charges;
- (c) as required by the General Manager, a long-stay report in the prescribed form;

- (d) a list of out-patients in the prescribed form, in duplicate, when the form is filled in, or not later than the twenty-fifth day of each month, whichever is the sooner;
- (e) monthly operating statements and financial and statistical returns in the prescribed form as required by the General Manager; and
- (f) within thirty days after an in-patient is admitted as the result of an accident or at the time of discharge, whichever is earlier, and for each subsequent admission, an accident report in the prescribed form.

58. (1) The General Manager may at any time and from time to time require a hospital to obtain from the insured person's attending physician and forward to the General Manager a written statement that the attending physician shall prepare regarding the condition of the insured person and stating the reasons showing the necessity for the insured services or other treatment provided during all or any part of his stay in hospital.

(2) Where a patient receives out-patient services, the attending physician shall prepare a medical record for the patient in the prescribed form within twenty-four hours after the services are provided.

(3) The General Manager may require a hospital to obtain from the insured person's attending physician and forward to the General Manager a written statement that the attending physician shall prepare regarding the condition of the insured person and stating the reason showing the necessity for any ambulance services authorized for such insured person.

Hospitals are required to send confidential information to the Ontario Health Insurance Plan under The Health Insurance

Act, 1972, but the disclosure involved is not mentioned in the legislation governing hospitals. Subsection 2 of section 33 of The Health Insurance Act, 1972 provides that "every insured person shall be deemed to have authorized his physician or practitioner who performed insured services to provide the General Manager with such information respecting the insured services performed...". Subsection 3 of section 33 also provides that "no action lies against a physician, practitioner, hospital or related health facility providing insured services or any member of his or its staff because of the furnishing to the General Manager information relating to insured services provided by him or it." Whether the disclosing institution has the 'implied consent' of the patient under section 33 of The Health Insurance Act, 1972, or simply the authority to make a non-consensual disclosure, this authorization should be reflected in the statute governing the release of confidential information maintained by hospitals and other health-care facilities.

The Ministry of Health also obtains diagnostic and treatment information about all hospital in-patients from the Hospital Medical Records Institute. HMRI is a private non-profit data processing organization which processes data on the in-patients of hospitals and produces statistical reports and indices for hospital use. A full description of HMRI is found elsewhere in this report. There it is recommended that the legislation governing hospitals expressly authorize the practice of releasing patient information to HMRI for data processing.

By section 39(1)(o) of The Public Hospitals Act, the Minister, subject to the approval of the Lieutenant Governor in Council, is empowered to "make such regulations with respect to hospitals as are considered necessary for...the reports and returns to be submitted to the Ministry by hospitals". The brief of the Ontario Hospital Association states that public hospitals "readily accept" the principle behind the provision empowering the Minister to make regulations to obtain returns and reports, but "are concerned about the manner in which it is sometimes implemented by the Ministry staff." The Ontario Hospital Association cites examples "of bureaucratic actions by Ministry officials which compromise the confidentiality of patient information by requiring hospitals to provide data, without making this the subject of regulation." The detailed patient identification required on some government forms creates an "invasion of privacy", and the Association asks that the regulations "and the forms resulting from them, be designed with a full consideration of the rights of patients to privacy, and...these rights be balanced against the assumed need of the government for statistical or other information."

It is possible to determine which and how much information is actually required for the purpose of each type of collection only with careful individual evaluation and study. The 1978 Report of the Ministry of Health Working Party on the Confidentiality of Health Records in Ontario also questioned whether the Ministry collects more patient-identifiable information than is necessary, and made the following recommendations with respect to its collection practices:

That the Health Information Review Committee expand their activities to define the objectives for Ministry information in order that information collection be limited to only those items that serve defined Ministry objectives and meet defined Ministry "needs".

That a review be made of all health records, forms, and information received or requested by the Ministry, and within the Ministry Information System in order to establish guidelines for the deletion of individual patient identification whenever and wherever feasible.

The Honourable Dennis Timbrell, the Minister of Health, made the following statements on this subject in the course of his October, 1978 address to the Canadian Health Record Association:

We recognize the need to define Ministry objectives more clearly, so the information we collect is limited to what is necessary. We are reviewing our systems to determine whether some of the data we obtain is not really necessary.

We also intend to review all forms and documents, to determine if the deletion of individual patient identification is possible.

In connection with the review of forms and documents, the Ontario Hospital Association made the following suggestions:

that the review body suggested by the Minister of Health to determine the necessity for health related information collected through his Ministry's forms and

documents, include representation from the public, the OHA and the OMA and that the review be given urgent priority.

This need for review of collection procedures is not limited to the Ministry of Health. Health-care facilities under the jurisdiction of the Ministry of Community and Social Services are also required to supply that Ministry with returns and reports. In a follow-up letter to its brief, the Ontario Hospital Association referred to a form letter sent by the Director of Family Benefits in this Ministry to hospitals requesting identifiable patient information in order to assess eligibility for family benefits. "It would appear", the Association said, "that if the form is filled out properly, there would be a breach of the rule of confidentiality." Moreover, it is not only the government's need for, and practices in, collecting confidential information which require re-evaluation. Its inspection and auditing of patient data in hospitals and health-care facilities have also caused concern.

Section 43 of The Health Insurance Act, 1972, as amended by S.O. 1974, chapter 60, section 8, provides for the appointment of inspectors in the following language:

43. (1) The Minister, from among persons nominated for such purpose by The College of Physicians and Surgeons of Ontario, may appoint in writing medical and financial inspectors with the duty and power to inspect, examine and audit books, accounts, reports and medical records maintained in hospitals and health facilities, offices of physicians and other health care facilities respecting patients who are receiving or who have received insured services, and such medical and financial inspectors shall act only at the direction of the Medical Review Committee.

(1a) The Minister, from among persons nominated for such purpose by a body referred to in section 5a that nominates persons for appointment to a practitioner review committee in respect of a health discipline, may appoint in writing practitioner and financial inspectors with the duty and power to inspect, examine and audit books, accounts, reports and records maintained in hospitals and health facilities, offices of



practitioners and other health care facilities respecting patients who are receiving or who have received insured services provided by or at the direction of one or more practitioners engaged in the practice of the health discipline in respect of which the practitioner review committee has been appointed, and such practitioner and financial inspectors shall act only at the direction of such practitioner review committee.

(2) No person shall obstruct a medical or practitioner or financial inspector in the performance of his duties under this Act and the regulations.

Although the relevant health-care facilities are required to allow access and make disclosures in accordance with The Health Insurance Act, 1972, section 48 of Regulation 729 under The Public Hospitals Act provides for information release only to appointees of The College of Physicians and Surgeons, and only for "the purposes of the College", not to them in their capacity as health insurance inspectors. Disclosure by those facilities covered by The Health Insurance Act, 1972 to a medical, practitioner or financial inspector designated under that Act for the purpose of audit or professional monitoring should be expressly referred to in the legislation governing the release of confidential information from these facilities.

Another type of government audit involving inspection of confidential patient information maintained by health-care facilities was the subject of comment by James A. Wakeford, the executive director of Oolagen Community Services, a designated psychiatric facility under The Mental Health Act. The confidentiality and disclosure of information from its patients' clinical records is governed by section 26a of that Act, which makes no provision for the disclosure of information to a government inspector. However, under section 4 of the Act, officers designated by the Minister of Health are provided with the power to inspect confidential documents:

4. (1) The Minister may designate officers of the Ministry or appoint persons who shall advise and assist medical officers of health, local boards of health, hospitals and other bodies and persons in all matters

pertaining to mental health and who shall have such other duties as are assigned to them by this Act or the regulations.

(2) Any such officer or person may at any time, and shall be permitted so to do by the authorities thereat, visit and inspect any psychiatric facility, and in so doing may interview patients, examine books, records and other documents relating to patients, examine the condition of the psychiatric facility and its equipment, and inquire into the adequacy of its staff, the range of services provided and any other matter he considers relevant to the maintenance of standards of patient care.

Oolagen Community Services is also a children's mental health centre under The Children's Mental Health Services Act, 1978, an Act administered by the Ministry of Community and Social Services, which provides for programme advisers who have the power to inspect "records":

9. (1) The Minister may designate in writing any person to be a program adviser with such powers and duties for the purposes of this Act and the regulations and subject to such limitations, restrictions, conditions and requirements as the Minister may set out in the designation.

. . . . .

(3) A program adviser may at all reasonable times and, upon producing proper identification,

- (a) enter any children's mental health centre and inspect the facilities, the services provided and the books of account and other records therein; and
- (b) inspect the books of account and other records of an approved corporation that pertain to a children's mental health centre.

(4) Every person when requested so to do by a program adviser shall permit the entry and inspection by the program adviser of the premises referred to in subsection 3 and shall produce and permit inspection of the books of account and other records therein and supply extracts therefrom.

(5) No person shall hinder or obstruct a program adviser in the performance of the program adviser's duties or refuse to permit the program adviser to carry out such duties or refuse to furnish the program adviser with information or furnish the program adviser with false information.

A health-care facility such as Oolagen, subject to both of these Acts, may experience inspectors appointed under legislation administered by both Ministries seeking access to confidential patient information. This exposure to more than one requirement for inspection is by no means unique to a children's mental health centre, as The Public Hospitals Act, The Community Psychiatric Hospitals Act, and The Private Hospitals Act all provide for inspectors or advisers for their own purposes. In his submission Mr. Wakeford said, "it is certainly not clear in law as to which government officials, under which conditions, should have access to what information (records) in the Children's Mental Health Centre." He went on to question the permitting of access to sensitive medical documents by auditors:

We are not convinced auditors should have the right to see client's records...We have been trying to find a compromise and to this end we have had our lawyers prepare consent forms to permit the auditors to see client records if the client agrees. I must confess, however, to some reservation that clients may feel some tacit pressure to sign such consents. There also remains the question of competence of auditors to interpret in a meaningful way clinical diagnoses.

A similar concern was expressed by the Ontario Medical Association in its brief. The Association did not refer to auditors from the Ministries but rather to the right of the Provincial Auditor, in performing a financial audit under The Audit Act, 1977, to inspect sensitive patient files in the course of the audit. Under The Audit Act, 1977, S.O. 1977,

chapter 61, the Provincial Auditor's right of access is referred to in the following sections:

13. (1) The Auditor may perform an inspection audit in respect to a payment in the form of a grant from the Consolidated Revenue Fund or an agency of the Crown and may require a recipient of such payment to prepare and to submit to the Auditor a financial statement that sets out the details of the disposition of the payment by the recipient.

(2) No person shall obstruct the Auditor or any member of the Office of the Auditor in the performance of an inspection audit or conceal or destroy any books, papers, document or things relevant to the subject-matter of the inspection audit.

. . . . .

14. The Auditor may examine any person on oath on any matter pertinent to any account subject to audit by the Auditor or in respect of any inspection audit by the Auditor and for the purpose or such an examination the Auditor has the powers conferred upon a commission under Part II of The Public Inquiries Act, 1971, which Part applies to the examination as if it were an inquiry under the Act.

The brief of the Ontario Medical Association questioned a financial auditor's need for confidential medical information in the performance of his duties and the propriety of allowing non-medical personnel to have access to information of that kind. The following are the relevant points from the Association's submission:

38. We believe that financial auditors can and must accomplish their work without perusing confidential medical records.

39. The opening of medical records to yet another class of civil servants is contrary to the public interest, and flies in the face of resentment over breaches of

confidentiality which brought about this Royal Commission.

40. The Ontario Medical Association is unalterably opposed to the opening of medical records to financial inspectors or other non-medical personnel.

Recommendation No. 4:

That the Audit Act be reviewed and if necessary amended to ensure that the Provincial Auditor and his staff do not have access to confidential medical records.

The Public Health Service of the U.S. Department of Health, Education and Welfare published general provisions for the "Confidentiality of Alcohol and Drug Abuse Patient Records" which require that levels of access to sensitive health information for audit or evaluation purposes reflect the qualifications of the inspector to receive it:

Governmental agencies.-Rules.

(a) In general. Where research, audit, or evaluation functions are performed by or on behalf of a State or Federal governmental agency, the minimum qualifications of personnel performing such functions may be determined by such agency, subject to the provisions of this part, with particular reference to the organizational requirements and limitations on the categories of records subject to review by different categories of personnel.

(b) Financial and administrative records. Where program records are reviewed by personnel who lack either the responsibility for, or appropriate training and supervision for, conducting scientific research, determining adherence to treatment standards, or evaluating treatment as such, such review should be confined as far as practicable to administrative and financial records. Under no circumstances should such personnel be shown caseworker or counsellor notes, or similar clinical records. Programs should organize their records so that financial and



administrative matters can be reviewed without disclosing clinical information and without disclosing patient identifying information except where necessary for audit verification.

The U.S. House of Representatives Committee on Government Operations, in its March, 1980, Report on Bill H.R. 5935, the "Federal Privacy of Medical Information Act", commented on the difficulty of, and the need for, the evaluation of government requirements for information concerning the patients of health-care facilities:

Where a government agency does not need patient information, the right to obtain that information should be restricted. However, that decision must be made on a program-by-program basis. The committee suggests that as each federal health program comes up for revision or reauthorization, its information needs should be reevaluated and statutory limitations should be imposed whenever appropriate. However, such restrictions can only be imposed after thorough study.

In Ontario there is an obvious need for each category of government recipient to thoroughly review its requirements and procedures with respect to confidential patient information from health-care institutions.

Legislation dealing with the confidentiality of information maintained by hospitals and health-care facilities should properly and specifically designate every recipient authorized to receive confidential information without patient consent. Every government recipient's right of collection and inspection should be designated thereunder, subject to the conditions and limitations on disclosure and use set out in the report to the Deputy Minister required in the recommendation that follows:

*Recommendations:*

75. *That legislation providing for the collection, audit or inspection of confidential patient-identifiable information maintained by hospitals and health-care facilities by government recipients require that every category of government recipient conduct a review on a periodic basis and report to the Deputy Minister*

of Health or his designate with respect to:

- (a) the purpose and objective in obtaining this information;
  - (b) the method used to achieve the purpose, to determine if it is the least intrusive possible. (Methods of achieving the purpose without using patient-identifiable information should be sought. Consideration should be given to employing persons with medically-oriented training or qualifications in positions with a high frequency of exposure to sensitive medical information);
  - (c) the quantity, quality and use of the information obtained, to determine if practices are consistent with the stated requirements; and
  - (d) the procedures in place to safeguard the confidentiality of the information and to provide for its prompt destruction, including a retention schedule and logging and destruction procedures.
76. That legislation governing the confidential information maintained by hospitals and health-care facilities permit the disclosure of health information to prescribed government recipients authorized to collect, audit or inspect confidential information under provincial legislation.

#### The Public Institutions Inspection Act

An inspection panel under The Public Institutions Inspection Act, 1974, S.O. 1974, chapter 64, has the civil function of the now abolished grand jury to inspect institutions maintained by public funds, with the extended power to inspect documents and interrogate persons on the premises. Sections 2 to 6 of the Act provide as follows:

2. (1) The judge of every county or district shall, on the first Monday in May and November each year, or so soon thereafter as is practicable, convene in open court a public institutions inspection panel composed of seven persons selected from the jury roll prepared under The Juries Act, 1974 for the county or district and for this purpose the sheriff shall provide the panel.

(2) The Juries Act, 1974 applies to the selection, recording, summoning, attendance and service of the persons for service on a public institutions inspection panel in the same manner as to the selection, recording, summoning, attendance and service of persons for service on a panel of jurors selected for a sittings of a court.

. . . . .

4. (1) The panel may inspect all or any of the institutions in the county or district that are maintained in whole or in part by public money.

(2) The panel shall inspect all institutions in the county or district in which persons are being held in custody, for the purpose of a judicial proceeding.

. . . . .

5. (1) Subject to any agreement between the chairman and the institution, the panel may, after a request for entry by the chairman, enter any public institution the panel is entitled to inspect under section 4 at any time during reasonable business hours and may inspect therein all parts of the premises, and any documents, records, files or accounts in the custody of the institution, and the panel or any member thereof may interrogate any person on the premises concerning any matter respecting the affairs, administration and operation of the institution.

(2) Any person who wilfully obstructs an inspection by a panel or any member thereof under subsection 1 is guilty of an offence and on summary conviction is liable to a fine of not more than \$5,000 or to imprisonment for a term of not more than one year, or to both.

6. (1) The panel shall submit its report to the judge sitting in open court.

(2) The judge to whom a report is submitted shall forward a copy of the report to the Attorney General.

(3) The report submitted to the judge shall be filed with the clerk of the county or district court as a public document and shall be available for public inspection.

The brief of the Ontario Hospital Association contained the following comments about this Act:

When the Public Institutions Inspection Act, 1974, was being processed by the government, the Association was very concerned that it appeared to give members of a public inspection panel freedom to examine patient medical records. Although we were not successful in obtaining an amendment preventing access to medical records, the matter was clarified by the Hon. Roy McMurtry, Attorney General, by letter dated February 2, 1976, to the effect that a hospital should not allow panel members to inspect medical records.

The Attorney General's letter referred to above read, in part, as follows:

It is the opinion of the Ministry that the specific provisions of section 48 of Regulation 729 which imposes a duty on boards to secure the confidentiality of medical records takes priority over Section 5(1) of The Public Institutions Inspection Act. In these circumstances, the employee of a hospital charged with providing for the security of the medical records should

refuse to permit the inspection of such documents. This would be the due process unless and until the panel has obtained an order or other process from the county or district judge permitting the panel to inspect the documents.

The refusal by such a hospital employee to permit the inspection of a patient's medical records by the panel would not, in our opinion, be considered a wilful obstruction of a panel in its duties. This is due to the fact that the refusal is in compliance with section 48 of Regulation 729.

William C. Jappy, the director of the Psychiatric Hospitals Branch of the Ministry of Health distributed a memorandum dated December 10, 1976, to the administrators of all provincial psychiatric hospitals, disputing the public institutions inspection panel's right of access to the confidential patient information held by the facilities under his jurisdiction:

The potential actions of this panel have serious implications for our psychiatric facilities and to this end all Administrators are advised that if they deem it necessary they may refuse access of their records to this panel.

The patient's right to confidentiality of information is still the primary concern of this Branch.

If challenged, you can argue that this Act does not bind the crown. If unsuccessful, you can fall back on the view that the duty of confidentiality in The Mental Hospitals Act takes priority over The Public Institutions Inspection Act.

In my view the Attorney General's opinion and Mr. Jappy's instructions make a recommendation on this issue unnecessary.

#### The Canadian Council on Hospital Accreditation

The Canadian Council on Hospital Accreditation was incorporated under federal law in 1958 and given the authority "to conduct a survey and accreditation programme for Canadian



hospitals", including the establishment of standards for hospital operation and the recognition of a hospital's compliance with these standards by issuing a certificate of accreditation. Participation of hospitals in this programme is voluntary. The purpose of the accreditation is, essentially, "to promote a high quality of medical and hospital care in all its aspects" by encouraging both the application of basic principles of efficient patient care, and the maintenance of essential diagnostic and therapeutic services in the hospital.

The present practice is for health-care professionals, appointed by the Canadian Council on Hospital Accreditation, to visit hospitals which have requested accreditation or a renewal of their accredited status to inspect and evaluate hospital compliance with accreditation standards. The examination of medical records is a necessary part of the accreditation process since the inquiry is concerned with the quality of all types of care administered by a hospital, as well as the adequacy of its organizational, administrative, and record-keeping procedures.

The Council's 1977 Guide to Hospital Accreditation contains the following clause which requires a hospital to authorize the Council's access to confidential documents:

In submitting its application for accreditation survey, the hospital shall authorize the Council to review official records and reports of public or publicly recognized licensing, examining, reviewing or planning bodies, as well as patients' clinical records and minutes of the hospital and medical committee activities.

However, in Ontario, a health-care institution has no legislated authority to permit the examination of medical or clinical records by the Canadian Council on Hospital Accreditation. The Ontario Hospital Association made the following submission:

Until now it has not been considered necessary to specify in section 48 [of Regulation 729] that access by accreditation surveyors to medical records is permissible but we believe formal authorization is now desirable.

The hospital accreditation process is invaluable. It should be authorized and governed by the provisions applicable to audit procedures generally.

*Recommendation:*

77. *That access to confidential patient information by the official representatives of accreditation surveyors for the purpose of granting or reviewing accreditation be permitted under legislation governing hospitals.*

Federal Health-Care Facilities

In Ontario, the federal government operates five hospitals, twelve nursing stations and the National Defence Medical Centre, providing care for persons under federal jurisdiction, including the Indian and Inuit population, and members of the armed forces. In many parts of Ontario, particularly northern Ontario, residents of Ontario, whether under federal jurisdiction or not and whether they are native or non-native, have equal access to both federal and provincial health-care facilities. One federal hospital, the Sioux Lookout Zone Hospital, is the focal point of a programme sponsored by The Hospital for Sick Children, the Faculties of Medicine and Dentistry of the University of Toronto in collaboration with the Medical Services Branch of the Department of National Health and Welfare, offering medical services to a wide area of Northern Ontario. Medical care provided by a federal health-care facility is paid for by the Ontario Health Insurance Plan.

There are no statutory provisions to protect the confidentiality of health information maintained by these federal facilities. Patient information in these health-care centres does not come within legislation enacted by the province. I am confident that the Department of National Health and Welfare is prepared to co-operate with the Province and to require the same minimum standards of confidentiality protection for the patients of its health-care facilities in Ontario as are required for the institutional health-care providers under provincial jurisdiction.

*Recommendation:*

78. *That the Government of Ontario request the Federal Government to adopt for its health-care facilities operating in Ontario the same minimum requirements for protecting the confidentiality of patients' health information as is found in Ontario provincial legislation.*

## Individual Health-Care Providers

Ethical and legal support for the concept of confidentiality with respect to health information concerning patients is expressed in the codes of ethics and statutes governing the various health-care professions and occupations. One can trace the standard of confidentiality expected of physicians to ancient Greek medicine. The "Physician's Oath", attributed to Hippocrates and still respected by members of the medical profession, contains this statement in one of its translations:

All that may come to my knowledge in the exercise of my profession or outside of my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and will never reveal.

A more modern version of this traditional affirmation of the principle of confidentiality is contained in the Code of Ethics of the Canadian Medical Association, which has been adopted by The College of Physicians and Surgeons of Ontario:

The ethical physician...will keep in confidence information derived from his patient, or from a colleague, regarding a patient and divulge it only with the permission of the patient except when the law requires him to do so;

A further refinement is found in Regulation 577/75-Medicine, made under the authority of The Health Disciplines Act, 1974, S.O. 1974, chapter 47:

26. For the purpose of Part III of the Act,  
"professional misconduct" means,

. . . . .

21. giving information concerning a patient's condition or any professional services performed for a patient to any person other than the

patient without the consent of the patient unless required to do so by law;

The principle has been recognized in our highest court. In Halls v. Mitchell, [1928] S.C.R. 125, [1928] 2 D.L.R. 97, Mr. Justice Duff, speaking for the majority of the Supreme Court of Canada said, at page 138:

It is, perhaps, not easy to exaggerate the value attached by the community as a whole to the existence of a competently trained and honourable medical profession; and it is just as important that patients, in consulting a physician, shall feel that they may disclose the facts touching their bodily health, without fear that their confidence may be abused to their disadvantage.

In addition to physicians, other health-care providers who fall within The Health Disciplines Act, 1974 are governed by definitions of professional misconduct which reflect the importance attached to the maintaining of confidentiality.

#### Dentistry - Regulation 576/75

36. For the purposes of Part II of the Act, "professional misconduct" means:

. . . . .

- (29) giving information concerning a patient's dental condition or any professional services performed for a patient to any person other than the patient without the consent of the patient unless required to do so by law;

#### Nursing - Regulation 578/75

21. For the purposes of Part IV of the Act, "professional misconduct" means:

. . . . .

- k. failure to exercise discretion in respect of the disclosure of confidential information about a patient;

Optometry - Regulation 585/75

26. For the purposes of Part V of the Act,  
"professional misconduct" means:

. . . . .

21. Giving information concerning a patient's vision to any person other than the patient without the consent of the patient unless required to do so by law.

Pharmacy - Regulation 579/75

47. For the purposes of Part VI of the Act,  
"professional misconduct" means:

. . . . .

- (x) conduct or an act relevant to the practice of a pharmacist that, having regard to all the circumstances, would reasonably be regarded by members as disgraceful, dishonourable or unprofessional.

By-law 11 of the Ontario College of Pharmacists is the Code of Ethics, section 6 of which is as follows:

A pharmacist should respect the confidential and personal nature of his professional records; except where the best interest of the patient requires or the law demands, he should not disclose such information to anyone without proper patient authorization.

Members of other health professions and occupations are also required to observe the principle of confidentiality. A few examples follow.

Regulation 42/75 made under the authority of The Denture Therapists Act, 1974, S.O. 1974, chapter 34:

7. For the purposes of the Act, "professional misconduct" means:

. . . . .



26. giving information concerning a patient's dental condition or any service performed for a patient to another person other than the patient without the consent of the patient, unless required to do so by law;

Members of the Ontario Physiotherapy Association are governed by the rules of conduct of the Canadian Physiotherapy Association which provide as follows:

#### 4. Confidential Information

- (a) The member shall treat as confidential all information regarding a patient.
- (b) Relevant information regarding a patient may be communicated to members of the health team who are involved in the patient's treatment.
- (c) In situations where information is sought concerning the condition of a patient, unless a member is obliged by law to disclose such information, the member should:
  - (i) supply information about a patient only upon receipt of a signed direction from the patient and upon receipt of a written request from the person seeking information;
  - (ii) keep all signed requests and releases on file;
  - (iii) check the authenticity of requests with the patient, if there is any doubt;
  - (iv) never give information verbally.

The standards of professional conduct adopted by the Ontario Board of Examiners in Psychology include this statement as Principle 7:

Psychological service units shall maintain and protect records so that the privacy of the client is assured.

Without restricting the generality of the foregoing, the following interpretations are given:

. . . . .

7.3 A psychologist shall make available client information or records, as defined in Appendix C, only to those within the psychological service unit and to those professionals within a sponsoring institution who have a need to know in order to serve the client.

7.4 Subject to interpretation 7.3 above, a psychologist shall not release the name of a client or information regarding a client, or records as defined in Appendix C except with the informed written consent of the client or legal representative or guardian of the client except as directed by law.

The obligation of confidentiality expected of physicians is expressed in absolute terms and permits the disclosure of information without the consent of the patient only where it is required by law. It will be observed, however, that the provisions with respect to some other health-care providers allow for greater freedom or flexibility on the one hand, but present difficulties on the other. Nurses, for example, must "exercise discretion in respect of the disclosure of confidential information about a patient." But permitting the use of discretion prevents the application of uniform standards. Moreover it makes inter-professional conflict possible. We have seen conflict in the public health sector as it relates to students in schools. This subject is dealt with at some length elsewhere in this report.

## Physicians

There is no question that among physicians there is universal acceptance of a need for confidentiality. The brief of The College of Physicians and Surgeons of Ontario puts the position this way:

In the taking of a history and examining the patient, the doctor is entrusted with information of the most intimate and personal nature. The patient is willing to accept such an examination and inquiry, in a relationship of confidence and trust, to obtain the benefit of the physician's advice and treatment. It is unlikely, however, that anyone would disclose intimate details of their own life and that of their families if there was reason to believe the information would not be kept secret. Indeed, it is not difficult to think of situations where it would be unlikely that a physician would even be consulted if there was no assurance of confidentiality.

As we have seen, the physician's duty of confidentiality is qualified by the recognition that, where "required to do so by law", the physician is relieved of the obligation. This exception, though, is obviously of some concern to physicians, both with respect to legislation which is intended or interpreted as creating a legal obligation on the part of the physician to reveal confidential medical information (for example, various provincial audit provisions which are deemed to apply to, or are specifically directed to, access to physicians' and hospitals' medical records) and with respect to those exceptional cases that arise from time to time in which the legal requirement for disclosure is not certain but which might make desirable some option for the exercise of a discretion to disclose on the part of the physician. This concern was also expressed in the brief of The College of Physicians and Surgeons of Ontario:

Risks to a third party, or to society at large, weigh heavily on the conscience of a physician. It is difficult to know whether threats of injury to others will be carried out unless appropriate warnings are given. Similarly, to what extent is a physician expected to go to prevent an individual from inflicting injury to himself? Apart from these considerations, there are the risks to the safety of others presented by the commercial pilot with heart disease, the surgeon with failing vision, and the crane operator who experiences blackouts.

By way of background to the discussion that follows I shall give a number of examples of actual departures from the

principle that should have been respected. These examples came to our attention during our inquiry into the practices carried on by private investigators who sought confidential information on behalf of casualty insurance companies without the patients' authorization and acting in interests opposed to those of the patients. A detailed examination of these practices appears elsewhere in the report. The evidence shows that, over the years, confidential patient information has been released to investigators by the office staff of physicians, and on many occasions, by physicians themselves. Although in some cases the information was disclosed in response to the use of pretexts, on many other occasions no pretext was necessary, and the inquirer could rely solely upon the indiscretion and carelessness of the physicians or their employees.

In this connection, the extremely sensitive nature of the material that may in fact be recorded as part of a medical record should be borne in mind. The brief of the Ontario Medical Association contains the following statement:

Traditionally, medical records contained the physician's candid comments about the patient and his condition. These comments assisted the physician in recalling, months or years later, the precise circumstances surrounding the patient's physical and mental state....

Statements made by a patient in distress may be inaccurate, totally erroneous and highly inflammatory, and should remain as private communications between patient and physician.

The submission of Dr. T. P. Morley, professor and chairman, Division of Neurosurgery, University of Toronto, expressed concern with respect to authorized access to physician records:

In disability insurance cases, for one example, the signed authorization allows photocopying and unlimited dissemination by the insuring company. Furthermore, the patient has no idea whatsoever what is in his hospital records. On countless occasions I have had to advise the patient not to allow his hospital record to be copied for an insurance company because of the disclosure of entirely personal secrets irrelevant to the company's requirements. Neither

patients nor hospital records staff nor most doctors appreciate or feel strongly about this...

Apart from dissemination of irrelevant secrets, doctors' records concerning relevant aspects of a patient's illness are often entirely incomprehensible or frankly misleading to a recipient if he be an insurance company, a lawyer, or another doctor. Good medical records contain nuances and impressions, gossip and scutternut; all these notes help the doctor to form a final opinion of the patient, body and soul. These notes should be as inadmissible as an instrument for judging, say, an insurance claim, as hearsay evidence is in court. The only valid record for third party eyes is a formal report by the attending physician based on his knowledge of the patient.

Dr. Morley's comments have particular relevance to unauthorized and indiscreet disclosures.

The following extracts from private investigators' reports give some indication of the type of material that found its way directly from the files of patients' physicians into reports to insurance companies adverse in interest to those patients. The first two examples are from reports based on information provided directly by the physicians:

Example #1

The investigator subsequently contacted Dr. L who is the Claimants' family physician.

The investigator discreetly disclosed from the doctor the following information relating to both of the Claimants.

Mr. and Mrs. X were in an automobile accident about a year and a half ago and he hasn't as yet worked from this accident and he complains of a chronic low back pain and...actually that's a lie, he is finally back to work. He complains of low back pain, but he ascribes most of his



low back pain to the time that he went over the handlebars of his bicycle and landed on his back. But since this accident, he had a lot of low back pain and he was working as a District Sunday Sun Paper Boy, for awhile, and he was on Welfare. He was on Welfare for about a year and a half. He just recently, apparently gone into a business with a friend of his, restoring cars.

Now, Mrs. X has got a long, long standing psychiatric history. She's been in the Mississauga Hospital innumerable times and she's been under Dr. P and she's been under other doctors. She rather unfortunately got hooked up with me a while back. There is a long standing social problem. They live in absolute squalor. They're dirty. He's an obese, just God-awful looking guy and she is always complaining about their sex life and I can imagine why. As I said, she has been depressed. She's made suicidal gestures. She cut her stomach the last time and ended up in Hospital. They have homemakers in there, all the time, and apparently its just absolute squalor. I have never seen their house.

I've been basically in the role of supportive with respect to their psycho-social problems.

I was treating the back for awhile. I had sent him, just because it was an automobile accident, he had normal x-rays and so on, of his back, but I sent him to see Dr. F who is an Othopod, out here, and he agreed that it was just 'a chronic fibrocytis' and there was nothing to do and it would settle down. So, I got that out of the way.

This Dr. F had also sent Mrs. X to a Urologist, because she is chronically dribbling and wetting her pants.

So you see, I don't get too involved because with these kinds of people, I get fed up with them because they are flitting around from here, there and everywhere. I never know what's going on. I find that I don't give them particularly great care, although I was talking and spending a lot of time with her about a month ago. But I have not seen her for about three weeks.

The investigator made further discreet inquiries and subsequently contacted Dr. K's office who is a surgeon.

The investigator was discreetly advised from the doctor's secretary that he has not seen Claimant No. 2 for at least ten years.

The investigator was advised that Claimant No. 2's father was a very good friend of the doctor's and also that Claimant No. 2's father had recently died of Carcinoma of the lungs.

The investigator made further discreet inquiries and was advised by the doctor that Claimant No. 2 was a tremendous problem to his father and also that Claimant No. 2 was an adopted child.

The investigator subsequently contacted Dr. P's office who is a psychiatrist. The investigator discreetly disclosed that Claimant No. 1 is a patient of the doctor's. The investigator was advised that no information could be released without proper written authority.

#### Example #2

During this time, the investigator also contacted Doctor S's office and discreetly learned that the doctor, who was a General

Practitioner, first examined the Claimant in July of 1972 for headaches. The doctor advised the investigator that he subsequently saw him again on October 2nd, 1972, then subsequently admitted the Claimant to the [Hospital] in regards to his headaches.

In [Hospital], it was diagnosed as a cerebellar tumour presenting with about a three month history of loss of balance, vertigo, vomiting as well as headache. At [Hospital] we did a pneumoencephalogram and an arteriogram and these showed a right cerebellar tumour.

He was transferred to [Hospital]. On October 9th, the tumour was removed by Doctor T and it turned out to be a fairly low-grade astrocytoma. Afterwards he did fairly well although he had right sided cerebellar signs that are pretty prominent - still staggers, he has trouble speaking, he's taken to be drunk most of the time by the cops and "stuff like that".

His brother, A, is in jail right now for heroin addiction and trafficking. I really don't know about [the Claimant]. He's a psychopath in some ways. He gets into trouble with "the cops" - all kinds of things. He had a real chip on his shoulder after having the tumour out because his girlfriend left him. His problems were really from his own self-pity, not as a result of the tumour or the operation. He had deficits at the time that were pretty bad - he could hardly walk or talk. But he's improved markedly, however, he's still a bit of a psychopath. He comes from a very psychopathic family. As I said his brother is a real "winner".

In April of 1973, there was a court case [the Claimant] was involved in. I think he was being sent to jail and I think he was claiming that he had a head injury. He was charged with trespassing after visiting his girlfriend that had left him. He got into a fight with new boyfriend. There was some question as to whether he had received a head injury at the time.

He was brought back to [Hospital] at that time to reassess his head injury. The physicians there thought most of his problems were psychiatric - related to drug abuse. They didn't find anything wrong with him discharged him on Stelazine.

When we had him in the Hospital initially, the big differential diagnosis was drugs. Some of his friends, while visiting him, left some mandrax in his hospital commode. He was telling us that he wasn't taking drugs and that was not the reason he was stumbling around so much.

I think he gets "nailed" with drugs all the time. "Cops" have charged him for driving problems because of his staggering. I really don't think he takes drugs. I don't think he took them even when he was brought back to [Hospital]. Psychiatrists at the time thought he was taking LSD. I don't think he does. He can't afford to. If he takes drugs, he'll fall over. His state is such that he only has half a cerebellum. Anything that will upset his balance will make him incapacitated, so he can't afford to take them. (The investigator inquired and was advised that Dr. S did not treat the Claimant for any head injury in December 1975. The

Claimant never mentioned anything to him.)

I last saw him about a week ago and he really had no complaints. I think his attitude has improved. He's not getting into as much trouble with "the cops" and so forth. Around 1973 - 1974 he had several car accidents and stole things - really "messed up" then.

He's still living on welfare and has tried to go back to retraining but never really managed to - for lack of motivation. He's worked at various odd jobs but nothing he's ever stayed with.

I, personally, am not really worried about him. I haven't seen any deterioration in him at all.

The investigator made further discreet inquiries but was unable to disclose any further information in regards to the Claimant's medical background.

The following excerpts are taken from another sampling of reports containing information obtained primarily from secretaries or nurses working in physicians' offices, with a few quotations directly from the physician involved. It should be pointed out that, of all the breaches of confidentiality in physicians' offices, as opposed to hospitals, examined in the sample of the 1,597 files which were studied, the largest proportion by far came, not from the physicians, but from their employees:

### Example #3

The investigator disclosed from the office of Dr. R, an Orthopaedic Surgeon, office located in [address], Hamilton, Ontario, that the doctor's summary and opinion of the Claimant's condition is as follows:

"The patient has spondylolisthesis. I felt that his pain was due to spondylolisthesis.



I think that it should be mentioned, for whatever value it is, that this guy is a little bit manipulative. He wants everything put right, but he does not want to spend anytime doing it.

In 1974-1976 he was working full days and then the latter part of that time he was working as a contractor and a manager.

The patient states that he can't sweep floors because he's afraid he will collapse, but he can go fishing and he can go boating. He has low grade back pain and he says that it is so bad at times that he has difficulty in smiling. Pain is aggravated by bending, working, lifting, physical strain, sustained sitting, coughing, sneezing. Relieved by sleep and pain pills.

He really isn't interested in having anything done. He wants to get better but he doesn't want physio, etc.

We had tomograms done, which confirmed the lesion. These tomographs done on February 7, 1977, showed 'bilateral defects through the pars intra-articularis of L-4.'

He's a pleasant fellow, he's heavy. I think he's a bit of schemer. He's not a realist at all.

The patient was last seen in May 1977 when the results of his x-rays were reviewed with him."

#### Example #4

The investigator then contacted the office of Dr. F, a Psychiatrist located at [address]. The investigator was informed that Dr. F has been seeing the Claimant for

almost a year for psychotherapy sessions. She comes into his office and talks over her problems.

His diagnosis is depression and increasing state of frustration which related to the family situation - the marital situation and the rather passive attitude of the Claimant in the face of the aggressive individual that she is married to.

The investigator was informed that the Claimant has since become much more confident, asserting herself and she has developed some hobbies and is taking part in art work and art therapy. There have been quite a few changes in her.

The following report was compiled by a particularly successful investigator who managed to obtain information from four physicians or their employees, before drawing a negative response from the fifth. This example is interesting because it can be assumed that the investigator used essentially the same approach in contacting each physician's office, and it is apparent that whether a pretext was used or not, there was at least one physician or physician's employee who remained sensitive to his or her obligation of confidentiality to the patient:

#### Example #5

The investigator, unable to disclose any further information in regards to the Claimant's employment, made discreet inquiries in relation to the Claimant's medical background and contacted Dr. P, the Orthopedic Surgeon.

The Claimant was seen by Dr. P only once on June 29th, 1976. She has been in a motor vehicle accident and was complaining of headaches and neck pain. She was referred to Dr. P by Dr. G, a General Practitioner. The Claimant was a medical/legal patient and Dr. P sent a report to her lawyer indicating that there was no point in seeing her again as there was nothing further he could offer.

Doctor P felt that only the passage of time would settle her complaints.

X-rays of the Claimant's thoracolumbar spine were normal. Doctor P did not prescribe any medication for the Claimant as she was already taking Diazepam and Synoquin.

The investigator, unable to disclose any further information from the office of Dr. P, subsequently contacted the office of Doctor M, a General Practitioner.

The investigator was advised that the Claimant has been seen by numerous doctors. She was treated by Dr. M for her motor vehicle accident and Dr. Pe treated her before that. Doctor Pe is another General Practitioner. The Claimant is now being treated by Dr. G and her file has been sent to his office. There are no medical records in regards to the Claimant at Dr. M's office.

The investigator subsequently discontinued and contacted the office of Dr. G, a General Practitioner.

The investigator was informed that the Claimant was originally treated by Dr. A, then went to Dr. Pe, then Dr. M, and then to Dr. G.

The investigator was advised that it is really quite comical because Dr. A and Dr. G share one office and Dr. M and Dr. Pe share another and the two offices are across the hall from one another in the same medical building.

Dr. G has been the Claimant's family doctor since June of 1976 and is still treating her primarily for back pain and insomnia because of this pain.

The Claimant was last seen on October 8th, 1976 for upper abdominal pain and recurrent back pain which was now worse. She had been seen previously on September 21st, 1976, for vomiting and upper abdominal pain.

It was disclosed that the Claimant had a nervous breakdown in March and April of 1976 and was seen by Dr. C, a Psychiatrist in Brampton. It was also learned that the Claimant had been treated by Dr. Pe prior to her motor vehicle accident for a occipital and frontal headaches and neck pains and the development later of lumbosacral back pain.

The Claimant was prescribed tranquillizers and mood elevators.

A letter within the Claimant's file dated May 1976, stated that "attempts at physiotherapy and even hypnosis tried by her psychiatrist had failed."

In relation to the Claimant's nervous problems, the investigator was advised that the Claimant has had many varied ailments.

The investigator was also advised that the Claimant's lawyer is unhappy with the medical report from Dr. P.

In a letter to the Claimant's lawyer dated July 27th, 1976, Dr. G stated,

She was improving but still bothered by low back pains and weakness of the legs. Examination showed no tenderness, normal straight leg raising and no neurological problems. Over the subsequent two months she still had mild pain, some days worse than others. Poor financial situation necessitates return to employment. Gradual improvement to normal is expected over the ensuing months.

Dr. G gave no specific diagnosis in this letter or anywhere else within the Claimant's file.

The investigator contacted the office of Dr. C, a Psychiatrist, located at [address], Ontario.

Dr. C has seen the Claimant on two occasions only: January 16th, 1976 and March 8th, 1976. There are no letters written by Dr. C within the Claimant's file, only the doctor's notes. Doctor C was treating the Claimant for reactive depression and an immature personality.

The investigator was unable to disclose any further information from the office of Dr. C without written authorization.

The investigator subsequently contacted the office of Dr. Pe, a General Practitioner and was also informed that no information could be obtained without written authorization.

The following excerpt indicates the wide diversity of medical information that may find its way into such a report prepared without the knowledge and consent of the patient. As in many of the other examples, the indiscriminate, unauthorized gathering of medical information resulted in the dissemination of information of the most sensitive nature with little or no relevance to the purpose for which it had been gathered:

#### Example #6

The investigator discreetly contacted Dr. R and was advised by the doctor's secretary that the Claimant was first seen in the doctor's office in January 1975 for a urethral discharge. He had been on penicillin. He had pain, discomfort and burning on voiding.

He was seen again on February 1976. The only note on that visit is that "patient improved", put on Nifuran at that time. Doing some drinking.

He was next seen in August 1976 for prostatitis. Note is also made at this time that he has been drinking. He was given some skin medication at that time by Dr. W.

He was seen again January 11, 1977 for multiple condylomata in the pubic region. Here note was made that there was no urethral papilloma.



Dr. R wrote a letter concerning this visit:

I saw this man who was having recurrent episodes of condylomata in the pubic region. He noted it some time ago. It was progressively getting worse. He didn't seem to have anything else wrong with him. He apparently had some type of warty condition before in the arms, around the neck, treated and was cleared up. No urinary problems. Denies venereal disease and wife does not have any problems in that way. Put on Pendophalen at that time.

He was last seen in our office and the only note on the file is that the condition is improved.

The following opinion was offered by a physician after a lengthy recounting of several years' treatment of his female patient, including treatment not related to her accident, and a discussion of a report prepared for the patient's solicitor:

Example #7

On a "off the record" basis, Dr. A advised that some of this lady's problems may be of an emotional nature. There apparently are some family problems. Dr. A indicated Mr.            has been bankrupt a number of times and this has been an emotional strain for Mrs.            .

It was not clear whether or not Dr. A was referring to Mrs.            when he then went on to say that he has patients who seem to fabricate aches and pains as an excuse to talk with him and it is only over numerous visits that the real problem comes out.

Some of the disclosures in the following examples are clearly scandalous, while others are merely informative:

### Example #8

The investigator subsequently disclosed that the Claimant's family doctor is Dr. D, office located in [address], Ontario.

The investigator contacted Dr. D's office and learned that the doctor had consultations with Dr. A following the Claimant's motor vehicle accident on July 6, 1976. A summary of this consultation is as follows: The Claimant was admitted from ER to OR. He acquired pain, swelling and deformity to right shoulder. He was found to have fractured neck of the humerus with marked displacement.

The investigator was advised that the Claimant was last seen by Dr. D on April 7, 1976 at which time his parents were concerned that the Claimant was drinking too much. The doctor did not refer the Claimant to a specialist in regards to this problem. In June 1972 the Claimant had x-rays of a bowel which showed no organic lesion.

The investigator was advised by the doctor's secretary that to her knowledge, the Claimant is an adopted child. She also believes that the Claimant moved from his parents' residence.

### Example #9

From the office of Dr. D, Orthopaedic Surgeon, located at [address], Ontario, the investigator was informed that there was a note on the chart stating that this was a medical-legal file and there were numerous letters to and from the lawyers to Dr. Z, Dr. J, Dr. C, Dr. D and several letters from the North York General Hospital.

The investigator, at this time, was unable to disclose any information from the letters.

The investigator did, however, disclose that there was an x-ray taken on July 12th, 1976

of the Claimant's lumbo-sacral spine, which reads as follows:

North vertebral alignment - no fractures identified. Faint radiolucency projected over posterior aspect of the sacrum. I think that there is a superimposed shadow and not a fracture.

The investigator was informed that the Claimant was first seen by Dr. D on January 12, 1977, at which time she was being seen for a cervical sprain. Dr. D intended to see her in a couple of months for this. The investigator was informed that the Claimant has a low pain threshold and her symptoms are psychogenically magnified.

The Claimant was last seen March 9th, 1977 at which time she was progressing from her cervical and neck injury which occurred in a motor vehicle accident, July 12th, 1976. The Claimant has been taking acupuncture and hypnosis, although it is foolish to argue with her about its success and should be done only under the supervision of Dr. S.

There was no further information available from the office of Dr. D.

From the office of Dr. C, Internal Medicine, [address], Ontario the investigator was informed that no information could be obtained without written authorization.

From the office of Dr. W, Neurologist, [address], Ontario the investigator was informed that the Claimant's file was not presently in the office as the Claimant had taken it with her to the Clinic. The investigator did, however, disclose that the Claimant's first diagnosis was Choreic Form Movements with Sydenham's condition in May 1977 or St. Vitus dance. She was then diagnosed as having polyneuritis, tremor and encephalitis and in December 1977 she was diagnosed as having dyskinesia.

There was no further information available at this time from the office of Dr. W.

From the office of Dr. J, Psychiatrist, [address], Ontario the investigator was informed that no information could be obtained without written authorization.

Example #10

The investigator made discreet enquiries in relation to the Claimant's medical background and contacted the office of Dr. B, a general practitioner, Rexdale, Ontario. During the conversation Dr. B stated,

I have been the patient's family doctor since 1968. She has not had any serious illnesses or health problems in the past, other than diabetes. She is a juvenile diabetic. She has been a difficult child at home. There have been numerous family problems, financial and emotional upsets, between her and her parents. More than the natural amount of rebellion that happens in many teenagers.

She had a recent accident on May 26, 1977. She had headaches following the accident. There is a big functional component with her. My opinion is that the headaches are due to the accident. I did not take any x-rays as I didn't think they were warranted. I didn't give her any type of therapy and she was not off work. I saw her on May 27, 1977, the day following the accident. My notes read that she was hit by a drunk driver apparently. She had aching in her neck and left shoulder, upper back, chest and headaches.

Certain movements of her neck were tender and painful and she was complaining of a headache. She might

warrant an x-ray of her cervical spine, but the fact that she was able to work indicated to me that probably these symptoms were not all that severe. I felt that it was a thing that would resolve spontaneously within a reasonable time. She is able to work and she wasn't complaining unduly the last time I saw her, which was on June 3, 1977. I really didn't think x-rays or therapy was warranted. She is on Entrophen and Diazepam which I believe Dr. G has put her on at some stage.

The investigator, unable to disclose any further information from the office of Dr. A, discontinued the conversation and contacted the office of Dr. G, the internist, [address], Toronto, Ontario. Dr. G informed the investigator that he has only treated the Claimant for diabetes, and nothing else and that no further information could be obtained without written authorization.

#### Example #11

Dr. A, [address].

The records at this location indicate the Subject was involved in a motor vehicle accident, was hit from behind, and has been complaining of pain in her neck and dorsal spine.

She was also complaining of pain in the epigastric region and Dr. A presumed this was a soft tissue injury sustained from the accident.

X-rays taken at Toronto Northwestern Hospital were only of the cervical spine.

After the Subject had been complaining of pain for some time, she was sent to the clinic for more x-rays and it was discovered that she had a compression fracture of D11.



She last saw Dr. A June 13, 1977.

The impression was given by Dr. A's secretary that the Subject was rather over-reacting to the problem and made a comment to the effect that older Italians tend to be difficult in their reaction to pain.

Example #12

Dr. D is treating the Subject for orthopaedic problems mainly to do with his right shoulder and right arm. This stemmed from an automobile accident some two years ago.

It was stated that the Subject has had his share of accidents but that none have been serious. The opinion was given that this injury has been "dragging on" as the Subject is trying to collect some money.

Conversation with the secretary at this location confirmed that the Subject had several accidents and was continually complaining about one or the other of them. The secretary dreads his attendance at the office, describing him as "an awful man who is always complaining."

Example #13

From the office of Dr. M, General Practitioner, [address], Ontario, the investigator disclosed that the Claimant is a 41 year old, divorced fireman, with the [Fire Department].

The Claimant suffered from back problems in 1968 and had x-rays taken at that time of the lumbo-sacral spine and pelvis - which were normal.

The investigator was informed that the Claimant had a fractured right rib in February of 1977, but was unable to obtain any further information in relation to this.

The Claimant has also complained of an aching left elbow in the past.

The Claimant underwent a complete physical examination in June of 1977 and was found to be completely normal.

The investigator was also informed that Dr. M treats quite a few firemen, as patients, and that some of them are quite heavy drinkers.

The investigator was unable to disclose if the Claimant himself, was a heavy drinker, but did disclose that the Claimant was apparently off work a great deal.

The investigator was informed that the Claimant had been referred to Dr. A, a Dermatologist and Dr. D, a General Surgeon, in the past.

No further information was available from the office of Dr. M without written authorization.

In none of the examples is there justification for the breach of the physicians' duty to their patients. Moreover, it would not be an acceptable explanation for a physician to say that he or she ought not to be held responsible for unauthorized disclosures made by an employee who was not subject to a code of ethics or The Health Disciplines Act, 1974. In my opinion, a physician is under a duty to ensure that his or her employees respect the obligation of their employer to protect the confidentiality of patients' records. A physician himself must be answerable for any violation that occurs in his or her office. Some of the abuses uncovered with respect to confidentiality have come about through thoughtlessness or carelessness, and must be eliminated by the simple exercise of vigilance and common sense.

Although the question of the nature of physicians' records is not within the scope of this inquiry, a comment on the subject is in order. A burgeoning literature on recent developments in medical record keeping reflects a constant trend to improved record keeping associated with improved patient care and a growing movement toward involving the patient in developing the medical record and maintaining its accuracy.

Quite apart from unauthorized disclosures of medical information, the increasing availability of health information from physicians' records for authorized and proper purposes is an

unavoidable development in our society. As a result the ethical physician must be aware that it can no longer be assumed that patient records will remain a private matter for himself or herself and his or her patient. Our investigation revealed some of the problems that can occur when sufficient care is not used in the preparation and development of medical records. The inclusion of faulty and erroneous material, questionable comments, and inaccurate assessments may, if released, even with authorization, to a third party, cause embarrassment to the patient, and seriously affect him or her socially and financially. In this connection, the submission made by Dr. Robert N. Richards, a specialist in dermatology, is appropriate:

...many of my colleagues and myself have, for many years, not put on our medical records any personal data (not essential to the medical case) which might in some way or form be damaging to the patient at a later date. Many use codes or symbols or phrases such as - "discussed personal problems". Shifting governments and the availability of computers and the need for financial checks make it clear that there CAN BE NO such thing as private medical records. Therefore, many of us in clinical practice, to protect our patients, simply do not record personal data unless it is absolutely essential to the case.

#### Examples:

- Case 1. A young man comes into the office complaining of a rash which could be produced by a drug. He states he is taking penicillin (the responsible agent), marijuana and aspirin. Since the marijuana is not essential to his case it would not be recorded on his chart.
- Case 2. A patient presents in the office with secondary syphilis. He has acquired this on an overseas trip and there is no chance whatsoever of tracing the contacts. The fact that the disease was contracted homosexually is not documented as again it is not essential to his management.

It is my belief as a clinician with several years experience that medical records cannot be private. I know many of my colleagues are doing the above (within the confines of the law and good medical practice)...

Government information requirements have a considerable effect on physicians' obligation of confidentiality. A physician may reveal information about a patient's condition or treatment without the authorization of the patient when required to do so by law. The occasions on which a physician is required by legislation to reveal particular patient information are, generally speaking, the exceptional events in his or her practice as, for example, in the case of the requirement to provide information with respect to venereal disease to the medical officer of health, or health information which relates to an individual's ability to drive to the Registrar of Motor Vehicles. However, universal government health insurance in Ontario makes necessary the disclosure of extensive information concerning patients' treatment and condition.

Section 33 of The Health Insurance Act, 1972, S.O. 1972, chapter 91, provides as follows:

33. (1) Every physician and practitioner who performs an insured service for an insured person shall provide the insured person, or the General Manager, with the particulars of his services and account that are required by this Act and the regulations or the General Manager for the purpose of payment of the claim.

(2) Every insured person shall be deemed to have authorized his physician or practitioner who performed insured services to provide the General Manager with such information respecting the insured services performed as the General Manager requires for the purposes of the Plan.

(3) No action lies against a physician, practitioner, hospital or related health facility providing insured services or any member of his or its staff because of the furnishing to the General Manager information relating to insured services provided by him or it.

Elsewhere in this report there is a detailed description of the processing of claims by the Ontario Health Insurance Plan. For present purposes, it is sufficient to point out that diagnostic information with respect to an insured medical condition is required, as well as a description of the particular service provided by the practitioner. It is thus apparent that the ethical requirement of confidentiality is subject to the requirements of The Health Insurance Act, 1972, so that physicians may document their diagnoses and treatment of their patients in order to be compensated under the Plan. Where an OHIP claim has been submitted on a patient's behalf, the legislation deems that the patient has authorized this disclosure of information. Most members of the medical profession seem to accept the necessity of some disclosure for the purpose of ensuring proper payment for services rendered as well as for the ancillary use of monitoring professional standards.

Access to patients' health-care records for the purpose of financial audit has been the cause of some concern within the profession in Ontario and in other jurisdictions because of the conflict between the value attached to medical confidentiality, on the one hand, and the social benefits to be derived from strict control of government expenditure, on the other. In its submission, the Ontario Medical Association indicated concern with respect to The Audit Act, 1977, S.O. 1977, chapter 61, and, acting on its solicitors' interpretation of the Act, advised its members "to refuse to show patients' medical records to the Provincial Auditor's staff or anyone else not authorized under The Health Insurance Act or The Health Disciplines Act to see them." The brief of the Association continues:

36. The Ontario Medical Association believes that sufficient access to medical and financial records in physicians' offices is provided in legislation governing medical practice and controlling criminal behaviour.

. . . . .

38. We believe that financial auditors can and must accomplish their work without perusing confidential medical records.

The Audit Act, 1977 provides as follows:

13. (1) The Auditor may perform an inspection audit in respect of a payment in the form of a grant from the Consolidated Revenue Fund or an agency of the Crown and



may require a recipient of such a payment to prepare and to submit to the Auditor a financial statement that sets out the details of the disposition of the payment by the recipient.

(2) No person shall obstruct the Auditor or any member of the Office of the Auditor in the performance of an inspection audit or conceal or destroy any books, papers, documents or things relevant to the subject-matter of the inspection audit.

(3) Every person who knowingly contravenes subsection 2 and every director or officer of a corporation who knowingly concurs in such contravention is guilty of an offence and on summary conviction is liable to a fine of not more than \$2,000 or to imprisonment for a term of not more than one year, or to both.

(4) Where a corporation is convicted of an offence under subsection 3, the maximum penalty that may be imposed upon the corporation is \$25,000 and not as provided therein.

14. The Auditor may examine any person on oath on any matter pertinent to any account subject to audit by the Auditor or in respect of any inspection audit by the Auditor and for the purpose of such an examination the Auditor has the powers conferred upon a commission under Part II of The Public Inquiries Act, 1971, which Part applies to the examination as if it were an inquiry under that Act.

Every employee of the Provincial Auditor is required to subscribe to an oath of office and secrecy which provides, in part, as follows:

...except as I may be legally required, I will not disclose or give to any person any information or document that comes to my knowledge or possession by reason of my being an employee of the Office of the Auditor.

Recent American decisions indicate that even though a state interest in monitoring the quality of health and medical care may outweigh the individual's right to privacy, and inspection of an individual's medical records may be necessary in the discharge of monitoring and audit duties, the method of accomplishing this purpose must, in itself, be subject to limitations. In Division of Medical Quality v. Gherardini (1979), App., 156 Cal. Rptr. 55, a decision of the California Court of Appeal, Mount Helix Hospital attempted to assert the statutory privilege or constitutional right to privacy of its patients to deny their records to the Division of Medical Quality of the Board of Medical Quality Assurance (Medical Board), a state agency within the Department of Consumer Affairs, State of California. The Board was carrying out an investigation of a physician and had served a subpoena on the hospital alleging gross negligence and incompetence on the part of the physician in the treatment of certain patients. It asserted that the medical records might afford evidence to substantiate the allegations. The subpoena did not indicate either patient consent or complaint and the hospital refused to surrender the records. The Court held that such a disclosure would only be compelled pursuant to an order drawn with narrow specificity in accordance with certain principles. At page 61, the following language is found:

...a governmental administrative agency is not in a special or privileged category, exempt from the right of privacy requirements which must be met and honored generally by law enforcement officials. To so hold is to ignore the federal and state constitutional commands as well as the numerous and persuasive judicial decisions in analogous areas. Moreover, such a premise focuses our attention only on the unquestioned right of the Medical Board to investigate the doctor; it ignores the patient's constitutional and statutory rights to be left alone.

The constitutional provisions here reviewed do not prohibit all incursions into the individual zone of privacy but rather require that any such intervention be justified by a compelling state interest. The resolution of these insistent issues involves a balancing of the respective interests and if state scrutiny is to be allowed, it must be by the least intrusive manner. [emphasis added]

In Hawaii Psychiatric Society, District Branch of the American Psychiatric Association v. Ariyoshi (1979), 481 F. Supp. 1028, Judge Wm. Matthew Byrne, Jr., of the U.S. District Court for the District of Hawaii considered certain sections of Hawaii's 1978 Medicaid anti-fraud law, in particular the one allowing government prosecutors to use administrative search warrants to inspect confidential psychiatric files. Judge Byrne held that there must be a reasonable suspicion that a particular health-care provider was defrauding the state before an inspection of sensitive records would be proper. Judge Byrne indicated his approval of a procedure by which the psychiatrist would go over files and delete confidential patient information, prior to reviewing with audit officials other information necessary to verify that services were performed in accordance with his billings. Although Judge Byrne did not doubt that the section in question was enacted in an effort to prevent fraud in the Medicaid programme, he decided that "the availability of this and other less intrusive means to achieve the compelling interest served by section 8 casts considerable doubt on that statute's constitutionality." Generally speaking, with respect to the powers needed to ensure that the Medicaid programme was not defrauded, he said, "There is no evidence that review by the State of personal and confidential information contained in a psychiatrist's patient files is necessary to prevent fraud. The details of a patient's problems are not necessary to an evaluation of whether a psychiatrist is rendering services in the amount claimed."

In Canada, there is, of course, no constitutionally guaranteed right to privacy, and in Ontario the privacy of medical files is protected by the legislative provisions that have been set out above. With respect to the broad authority granted either to a government agency for audit purposes, or the monitoring branch of a professional college, as in the case of the provisions in The Health Disciplines Act, 1974 relating to physicians and other health-care professionals, there is a conflict between the authority granted for audit or monitoring purposes and the obligation, subject to a legal requirement for disclosure of records, to maintain confidentiality. Patients do not have an interest that is separately considered and constitutionally protected from intrusive investigation. The confidentiality provisions applicable to individuals involved in auditing functions as set out in The Audit Act, 1977, or medical review under The Health Insurance Act, 1972, are not a complete answer to the expressed concerns. On the other hand, an outright refusal to disclose medical records to government and professional representatives who have a clear mandate to carry out in the public interest is inappropriate. However, it is surely desirable that the administrative procedures involved in

examining patients' records for monitoring and audit purposes be subject to guidelines that ensure that inspection is carried out in the "least intrusive manner."

Finally in this connection, I refer to the administrative procedures followed by the Professional Services Monitoring Branch of the Ministry of Health and the Medical Review Committee of The College of Physicians and Surgeons of Ontario with respect to referrals made by the General Manager of the Ontario Health Insurance Plan under section 22 of The Health Insurance Act, 1972, as amended by S.O. 1974, chapter 60, section 5(1), and S.O. 1975, chapter 52, section 4(1). That section reads, in part, as follows:

22. (1) Subject to section 24, the General Manager shall approve and assess claims for insured services, determine the amounts to be paid therefor and authorize the payment thereof in accordance with this Act and the regulations.

(2) Notwithstanding any action taken by the General Manager under subsection 1, where, in respect of insured services rendered by a physician, it appears to the General Manager on reasonable grounds that,

- (a) all or part of the insured services were not in fact rendered;
- (b) all or part of such services were not medically necessary;
- (c) all or part of such services were not provided in accordance with accepted professional standards and practice; or
- (d) the nature of the services is misrepresented,

the General Manager shall refer the matter to the Medical Review Committee and the Medical Review Committee may recommend to the General Manager that he pay, or refuse or reduce payment of, or require and recover reimbursement from the physician of any overpayment of, the amount otherwise payable and, subject to sections 24 to 28 and

subsections 3 to 9 of section 29, the General Manager shall carry out the recommendations of the Committee.

. . . . .

When a matter is referred to the Medical Review Committee by the General Manager of the Plan, a preliminary review is carried out by the administrative staff of the Committee. The letter of referral and supporting material are then presented to the Committee, which may decide whether further investigation should be carried out, or an inspection directed under subsection 1 of section 43 of the Act. On the other hand, the Committee may recommend to the General Manager that he pay the amount. In the case of an inspection or investigation, the Committee may subsequently proceed by inviting physicians to an interview or may direct full payment. If an interview is held, the Committee may decide either to refuse or reduce payment or direct payment in full. If payment is not to be made, a hearing must be held before making the recommendation to the General Manager. Sections 24 to 27 of the Act (as amended by S.O. 1974, chapter 60, section 6, and S.O. 1975, chapter 52, sections 5 and 6) provide for a hearing by way of appeal from the refusal of a claim by the General Manager to the Health Services Appeal Board.

Evidence was given at our hearings about the information provided to the Committee in the referral process and about the investigative role of the Medical Review Committee, and, more particularly, that of its administrative staff. The issues canvassed included the nature and extent of information provided by the Ministry of Health, the process by which the procedure for providing information was developed, and the uses to which the information has been put. Before the evidence was heard we received a letter from G. E. Fetherston, the General Manager of the Ontario Health Insurance Plan from April of 1972 to September of 1979, setting out the information given to the Medical Review Committee of The College of Physicians and Surgeons of Ontario. The letter reads, in part, as follows:

With reference to the Medical Review Committee of the College of Physicians and Surgeons, the following is a summary of information provided to them at their request and our agreement.



## FICHE FILES:

### 1. Claims Reference File:

Forwarded every two months and first sent in February 1977.

### 2. Practitioner Registry Files:

- a. Provincial Alpha Catalogue - practitioners registered in alpha sequence by name. Produced once per year, first sent July 1977.
- b. Provincial Numeric Catalogue - practitioners registered in numeric sequence by six digit I.D. number of groups by four digit I.D. number. Produced once per year, first sent January 1977.
- c. District Alpha Catalogue - practitioners by OHIP District Office and within District, alpha by name. Produced once every two months and first sent May 1976.

### 3. Daily Profile (Daily Distribution of Services):

This has been forwarded since the first month it became available. The first service month was April 1974, sent in December 1975.

Hard copies of items on the fiche may be prepared if necessary and examples of what is contained on the fiche are attached for the above three categories.

When a physician is referred by the Plan, certain information relating to the physician's practice is attached to the referral. The type of information depends to some extent on the reason for the referral. For example, there may be copies of verification letters received from patients indicating that the services were not provided. Copies of the relevant claims would be included.

There are generally included copies of a detailed claims analysis for a certain period, say a month, along with copies of all or part of the claims themselves for that month. The doctor's own profile covering a year of his activities is also attached.

The claims reference file is used by the Committee to check on services to subscribers by a referred physician for a period other than that covered by the specific information provided in the referral itself. In addition, during the Committee's investigation of cases concerning questions of medical necessity and acceptable standards of practice, it is vital for the Committee to be aware of services provided by other physicians to the patients of the physician under investigation. This can only be obtained from the claims reference file. Reference by the Committee to the file is often necessary and the provision of the fiche to the Committee eliminated the calls and submissions by the Plan of such information on a request basis.

The Registry files provide background information relating to a physician's option, specialty, etc. The physician's number is important since the claims themselves indicate the number only for a referring physician.

The enrolment fiche file is not forwarded to the Committee.

The other Practitioner Review Committees receive only the information provided with the referral itself.

Only the Medical Review Committee of The College of Physicians and Surgeons of Ontario receives the extensive material outlined in the letter. Other practitioner review committees receive much more limited material but it was explained at the hearings that 95 per cent of the referrals made by the General Manager of the Plan are, in fact, directed to the Medical Review Committee of The College of Physicians and Surgeons. It should also be pointed out that the general confidentiality provision in section 44(1) of The Health Insurance Act, 1972, as amended

by S.O. 1974, chapter 60, section 9, refers to the Medical Review Committee, as well as to other practitioner review committees, in connection with the preservation of secrecy of information relating to insured persons and insured services rendered which they have acquired in the performance of their duties under the Act.

On the subject of the amount of information given by the Health Insurance Plan to the Medical Review Committee, testimony was given at the hearings by Dr. John Carlisle, a Deputy Registrar of The College of Physicians and Surgeons and the secretary of the Medical Review Committee. He expressed the opinion that it was unlikely that the President and the Registrar of the College had been aware of the details of the information made available to the Committee before we inquired into the matter. The following extract from the transcript of the hearing discloses some of the concerns that were raised:

DR. CARLISLE: ...I think the reason for that is the affairs of the medical review committee are somewhat and quite distinct from those of the College and it is the policy of the general officers not to get too involved with what the MRC does because they are not supposed to know about the details of the MRC's considerations. For instance, MRC minutes are not spread around and so forth and so on.

MR. COMMISSIONER: But that policy is a policy which can easily be maintained even though the responsible officers of the College know in general terms how the committee operates and what information is available?

A. Oh, yes. I quite agree. I would also agree with your supposition that it may well be that they didn't. I don't know. I assume that you could well be right.

MR. STROSBURG: Doctor Carlisle, the concerns that I have are really one of the number of hats that you wear. On the one hand you have told us very frankly that you are involved doing preliminary investigation work with the discipline committee?

A. Which will eventually go to the discipline committee, yes.

Q. Yes. And that you have to make inquiries and that you work closely with the local authorities on occasions when you have to do that?

A. Occasionally, yes.

Q. That at the same time that you hold this position with the medical review committee where you have access to this enormous bank of information?

A. Yes.

Q. That you have on four occasions made a judgement that the public interest required that you access that information for a purpose other than an MRC purpose?

A. About that number, yes.

Q. Yes. The information that you hold is capable of being massaged into a very detailed profile about the physicians that you may have to investigate?

A. There is that capability, yes.

Q. The physicians generally who are represented by the College are unaware of this capacity?

A. Some of them are.

Q. Most of them are?

A. Well there is a pretty large association of them that publicizes their own newsletter that's, I think, much more aware of it than others. I...

Q. It's only recently they have become aware of it?

A. Well that might be fair to say, yes.

Q. Yes. You couple all of that with the fact that the senior people in the Ministry were unaware.

A. Well I don't know what goes on in the Ministry, Mister Strosberg.

Q. I am suggesting to you, Doctor Carlisle, that, when you look at all of those things, that it is really an unfair position to put you into to have to be responsible to have custody of all of that material and to have all of those varying responsibilities. Do you not agree?

A. It has its stresses.

Q. You have alluded to a group of physicians. Is it not the case that there is a group of people in the College that kind of think of you as really an investigator who is being overly zealous with the fulfilment of your functions?

A. I don't know whether they think I am being overly zealous. I think that they, I suffer from the inability by virtue of the limitations placed on me, and my committee suffers from the inability by virtue of the limitations placed on us in terms of confidentiality of what we do, of drawing to the attention of some of the members the very difficult types of circumstances that we have to deal with. In view of the fact that they don't know about the type of people that we are dealing with, they tend to assume that those types of activities are being applied to ordinary, normal, everyday doctors like themselves and they are very concerned about that.

MR. COMMISSIONER: Haven't you just put your finger on one of the chief problems of confidentiality? The public as a whole doesn't know and can't possibly be assured that breaches of confidentiality would only occur in the case of anti-social people, people for whom they would have no brief?

A. I quite understand your point.



MR. COMMISSIONER: But are they worried that the potential is there for them to be spied upon?

A. Yes, quite so.

MR. COMMISSIONER: Let me put my concern a little differently from the way in which Mister Strosberg has, and it has nothing to do with personalities or persons. A system which is designed in a way that would ensure that confidentiality will be respected has to be one which is workable no matter what persons are involved in its activities?

A. I would agree, Mister Commissioner. I think if the, no matter what system you have, if you assume that the top man is dishonest, no system can assure that the job will be done properly.

MR. COMMISSIONER: Right. So that if there is in fact in society an opportunity for persons with power to have access to all kinds of personal information which might be useful to them in the exercise of power... though when they are given the power they are all perfectly reputable, responsible, upright people, the system being there can be used by people who succeed them who don't have all those characteristics?

A. That's entirely right I think.

MR. COMMISSIONER: It may well be that under your direction there can be no abuse of the delicate information which is accessible to you, but your involvement is for a finite period of time. You are at some stage no longer going to be in that position.

A. I am sure that's right. Yes.

MR. COMMISSIONER: Someone else may not be as strong in his or her ability to resist the blandishments of other people--that's the wrong word--the requests of other people in the College to have access to this

information which would be useful for their purposes?

A. Yes. I think that's a fair thing to say.

MR. COMMISSIONER: Therefore shouldn't we be concerned with the principle of having that information where it is?

A. Yes, I think we should be concerned with the principle of having that information where it is. I only add to that that it seems to me that we are in addition dealing with competing social values and that I have to, in my own mind, for the purpose of my own thinking, I have to balance what I see as a very important social value in terms of maintaining the quality of care that we have in Ontario, which is high, against the confidentiality value.

MR. COMMISSIONER: Of course. That's the dilemma throughout the inquiry.

A. I realize that's your dilemma.

MR. COMMISSIONER: But can't you carry out that responsibility, even though with greater inconvenience, if the material is stored elsewhere? You are not precluded from carrying out your responsibility if the material remains where it is supposed to be under the statute, and that's with OHIP?

A. Okay. Let me answer that in the most honest manner that I can. Because it is a speculation and you understand that it is difficult. I will put it to you this way. In the way that we do it now, and I don't mean by the way we do it now referring to this information. I mean the method we adopt to handle what I'll loosely call peer review, I don't believe I could do the job without the information at my fingertips. That does not mean to say that I don't believe that we might not be able to re-organize the thing in some way. I don't know how now, but it might be possible.

Among the materials forwarded to the Medical Review Committee are the claims reference microfiche. The claims reference microfiche, their production, contents and distribution, are more completely described elsewhere in the section of the report describing the OHIP system. For present purposes it is enough to say that they contain on microfilm a summary, by OHIP number, of all OHIP subscribers and their dependants who have received services billed to OHIP over a fixed period of time, generally six months, along with diagnostic codes and fee schedule codes for those services. Because they identify patients, and describe their care and diagnoses, the claims reference microfiche are, and should be regarded as, the most sensitive file produced by OHIP. Dr. Gerald Gold, then Director of the Professional Services Monitoring Branch of the Ministry of Health, and Dr. Carlisle gave evidence about the course of events that led to the transmission to the Medical Review Committee of the various microfiche referred to in Mr. Fetherston's letter to us. An extract from the transcript of Dr. Gold's testimony at the hearings follows:

A. Perhaps a little bit of a background might be pertinent here. Up to approximately 1975 or 6, the volume of referrals to the medical review committee had initially been small in volume on an annual basis, but during '75 and '76 increased because of our abilities to, using the profile system to detect and pick out unusual patterns of practice. The fact that increasing numbers of cases were referred to the review committee meant that we were both involved frequently after the initial material was referred in providing additional materials to the committee during the course of their investigation of all these cases. To a point where an exceptional volume of our time and the medical review committee's time was spent simply in requisitioning and sending back additional materials. It was felt at that time that solely for the purpose of improving the operating efficiency of the committee that it would be best to have the committee obtain the fiche itself for the review committee's purposes.

Q. Well they never obtained it themselves. It always went through your office?

A. That's correct, sir.

Q. In the first instance did you speak with Mister Fetherston?

A. Yes.

Q. Did you tell him what you just told us?

A. Yes, sir.

Q. Did he agree that it should be sent?

A. He did.

Q. Was there any arrangement at that time made for the return of the fiche, the out-dated fiche?

A. No, there wasn't, sir.

Q. Was there any arrangement made for you to monitor the destruction of the fiche?

A. No specific arrangement made other than my understanding that the fiche was being destroyed.

Q. How did you have that understanding?

A. From conversations with Doctor Carlisle.

Q. Did you inspect the method of destruction?

A. No, sir.

Q. Did you require a written report to confirm that destruction?

A. No, I didn't.

Q. Is there any reason why you didn't?

A. No, sir.

Part of Dr. Carlisle's evidence was the following:

Q. Would you tell us please, when you first had a discussion with anyone about the possibility of the College receiving the claims reference file?

A. It was around the time of the changeover that I discussed this morning in the format of the daily distribution of services. When it became clear that the College was going to have to obtain at some expense microfiche readers and printers in order to carry on, we then discussed in conversations that I frankly cannot remember, but it was around that time, that if this expense was going to be entered into we should review the other materials which were available to determine what most efficient use could be made of that equipment and of our respective manpower resources. That included a discussion of the claims history file and the physician registry and all those other files that I mentioned.

Q. Do I understand you to be saying that until these discussions were precipitated by the problems as to the availability of the physicians daily distribution that there was no suggestion or discussion about the delivery of the claims reference file?

A. Not that I recall. No.

Q. It was only when the expense was being contemplated or had been incurred for the obtaining of these microfiche readers and printer that a discussion then was had as to the possibility of causing delivery to be made of the claims reference file?

A. I believe that's right. Yes.

Q. Who did you then discuss this matter with?

A. My recollection is that I discussed it with Doctor Gold. I think it was a telephone conversation, though it may have been a meeting. I cannot recall.



Q. Did you appreciate that the delivery of this file might be considered to be a matter of substantial policy concern to the Ministry of Health?

A. I think I can only say that I appreciated that it was a serious matter that needed consideration and I don't know what they consider a policy matter, so it is hard for me. I am not trying to weasel. I think the answer is basically yes, that we thought it was a serious matter and yes, we thought seriously about it.

W. Alan Backley and James B. S. Rose, who were Deputy Minister of Health and Assistant Deputy Minister, Administration and Health Insurance, respectively, both testified that they had been unaware of the decisions made by Mr. Fetherston at the request of Dr. Gold and Dr. Carlisle to distribute the various sets of microfiche to the Medical Review Committee.

After the hearing I was informed by the solicitor for the Medical Review Committee that the most sensitive information contained on the microfiche, the diagnostic code, was of little use to the Committee and that the file would be adequate for the Committee's purposes without it.

With respect to the uses to which the information given to the Medical Review Committee is put, Dr. Carlisle said that, as far as he knew, there had been no exchange of correspondence between anyone on behalf of the College and anyone on behalf of OHIP about the manner in which the College would handle the various microfiche, including how the microfiche were to be received, secured and eventually disposed of. Dr. Carlisle's testimony was very helpful on the subject of the occasions on which information from the microfiche in the possession of the Medical Review Committee had been used by persons other than the Medical Review Committee or its staff. The following is a summary of this evidence.

1. One of the matters agreed upon in 1977 was that the College should be permitted to examine the practitioner registration microfiche to obtain membership and other information about physicians. As the Medical Review Committee now had the complete practitioner registration microfiche, it was considered reasonable to provide this information directly to the College's registration department rather than sending weekly requests to OHIP for current addresses.

2. In connection with a matter which had been investigated by the police and which, at the time of the hearing, was before the courts, based, in part, on information provided to the police by OHIP, further questions had been put to the College by the police. Dr. Carlisle believed that several pages of physician distribution information may have been provided to the police to replace defective material received from OHIP.
3. In two instances in which the Executive Committee of the College believed that a serious danger to the public might be involved, the Registrar of the College had approached him concerning physicians in practice. The Registrar and Dr. Carlisle may have looked at the microfiche relating to the daily distribution of services of the physicians in question to ascertain whether they were actively practising, in order that action could be taken quickly if it proved necessary to intervene to prevent an incapacitated physician from performing surgery. It was Dr. Carlisle's position that, where public safety was involved, he would be prepared to use the daily distribution of physician services microfiche for a purpose other than that of the Medical Review Committee.

Although the purpose for which information from the OHIP master files is forwarded to the Medical Review Committee is to serve administrative convenience, the practice can be said to be authorized by subsections (2)(a) and (4) of section 44 of The Health Insurance Act, 1972:

44. (2) A person referred to in subsection 1 may furnish information pertaining to the date or dates on which insured services were provided and for whom, the name and address of the hospital and health facility or person who provided the services, the amounts paid or payable by the Plan for such services and the hospital, health facility or person to whom the money was paid or is payable, but such information shall be furnished only,

- (a) in connection with the administration of this Act, The Medical Act, The Public Hospitals Act, The Private Hospitals Act, The Ambulance Act or the Hospital Insurance and Diagnostic Services Act (Canada), the Medical Care Act (Canada) or the

Criminal Code (Canada) or regulations made thereunder;

. . . . .

(4) The General Manager may communicate information of the kind referred to in subsection 2 and any other information pertaining to the nature of the insured services provided and any diagnosis given by the person who provided the services to the statutory body governing the profession or to a professional association of which he is a member.

The existing and future provision of health information for audit and professional monitoring purposes should be governed by the following recommendation:

*Recommendation:*

79. *That legislation providing for the disclosure of health information for the purposes of audit or professional monitoring require that any person who obtains information for these purposes,*

*(a) remove or destroy information that enables patients to be identified where identity is not relevant or necessary to the investigation or, if identifiable information is necessary, at the earliest opportunity after the completion of the investigation;*

*(b) be prohibited from further use or disclosure of identifiable health information unless required by law or unless the information is required to relieve an emergency situation affecting the health or safety of any person;*

*(c) be required, on a periodic basis, to provide a report to the Deputy Minister of Health or his designate setting out,*

- (i) the purpose of the audit or monitoring;*
- (ii) how the information required is being used, to determine if practices are consistent with the purpose as stated and the legislative requirements for the audit or monitoring;*
- (iii) the method used to achieve the purpose, to determine if it is the least intrusive possible with respect to the use of identifiable patient information; and*
- (iv) the procedures in place to safeguard the physical security of identifiable patient information, including logging procedures, destruction procedures and a retention schedule.*

As the Code of Ethics now reads and the language of the regulation reflects, a physician may release information when required to do so by law and not be considered in breach of his obligation of confidentiality. Elsewhere in this report there is a full discussion of the various statutory requirements that may impose a duty upon a physician to report the condition of his patient, or information incidental thereto. These provisions include the reporting of medical conditions that might impair an individual's ability to drive, under The Highway Traffic Act, R.S.O. 1970, chapter 202, information that may lead to establishing child abuse, under The Child Welfare Act, 1978, S.O. 1978, chapter 85, communicable diseases under The Public Health Act, R.S.O. 1970, chapter 377, venereal diseases under The Venereal Diseases Prevention Act, R.S.O. 1970, chapter 479, and information about health services provided for the purposes of The Health Insurance Act, 1972. These measures require disclosure of health information and fall within the exception to the rule of confidentiality. In addition to these expressly permitted exceptions, circumstances sometimes arise in which there may well be a moral justification for behaviour which the language of section 26.21 of Regulation 577/75 characterizes as professional misconduct. During the course of our hearings, examples were given, not of violation of the regulation, but rather of compliance with the prohibition in circumstances in

which the physicians, in the opinion of most enlightened persons, should have made a disclosure despite the law.

Present in the examples to be described is a conflict between the obligation to the patient, as expressed in the ethical and regulatory requirement, and the public need for protection from threatened violence. There are two situations in which a physician may face an ethical dilemma, brought about by the absence of a legal requirement to release information, bringing him or her within the unambiguous statutory command to respect the confidentiality of his or her patient.

In the first situation, a request may be made to a physician for information concerning the mental or physical condition of a patient in connection with a crime in progress, in order to determine how best to approach a violent person in a way that would avert disaster. A helpful illustration was given at our London hearings by William B. Pogue, the executive director of the Woodstock General Hospital. In an incident that occurred a few years ago, the police in another jurisdiction in which an aircraft hijacking was taking place contacted the Woodstock police, who in turn communicated with the hospital. The individual involved had been treated at the hospital and information was provided to the police from his medical record. Acting on the basis of that information, the police were able to bring the hijacking to a satisfactory conclusion. Disclosure of information from the medical record in these circumstances is not permitted under the provisions of The Public Hospitals Act, R.S.O. 1970, chapter 378, or Regulation 729 thereunder, yet few would condemn the conduct under the conditions that prevailed. This example is typical of the kind of case in which a physician receives a request for information in his possession from an official who is in a position to describe the public risk involved.

The second type of situation does not involve a request by the police or any public official and the ethical dilemma is one in which the physician may be required to act purely on the basis of his own assessment of information about his patient. A physician may become aware of the commission of an offence, either because of the physical condition of, or an admission made by, a patient, in the latter case, perhaps during psychotherapy. Similarly, a physician may become aware of a threat of violence against another or others made by his or her patient. The brief of the ad hoc committee of the Department of Psychiatry at the University of Toronto dealt with this problem, and the following resolution of the dilemma facing the physician was suggested:



Where a patient informs his therapist of a serious crime he has committed or is about to commit, the therapist's responsibility to society (or the proposed victim) may override his duties toward his patient. Indeed it may be argued that it is in the patient's ultimate interest for the therapist to break confidentiality.

Prior to this he must assess the seriousness of the patient's threat or the truth of his claims.

If convinced that the patient is serious and cannot be dissuaded from a major criminal act, the psychiatrist has the responsibility to take all steps necessary to thwart the patient in his goal.

If the patient is suffering from a mental illness, the psychiatrist can certify him under The Mental Health Act and arrange for his immediate hospitalization. If this is to a closed setting, he may decide not to inform the police at that stage.

If he cannot get the patient to a hospital setting, he should contact the police, inform them of the patient's stated intentions and convey to them his certificate (Form I). He should also inform, or have informed, the proposed victim of the threat as he could be held responsible for avoiding to do this (N.B. Tarasoff case).

If the psychiatrist does not have grounds to certify the patient, he should inform the police and intended victim as before. He should also inform the patient of his intentions to disclose this information.

In the case of a confession by the patient of a serious offence already committed, the psychiatrist should attempt to persuade him to surrender himself to the police. Otherwise he should inform him that it is his social duty to divulge this information to the authorities.

The reference to the Tarasoff case is to the judgment of the Supreme Court of California in Tarasoff v. Regents of the University of California (1976), Sup., 17 Cal.3d. 425, 551 P.2d 334, 131 Cal.Rptr. 14, a judgment to be discussed later.

The following case is taken from the very helpful brief submitted by the London Police Force:

A recent case in London can be directly related to the dilemma a psychiatrist must face in the physician/patient relationship.

Russell Johnson and his wife were interviewed by a psychiatrist in 1969 in the course of which he informed the psychiatrist that he had broken into an apartment and sexually attacked a woman. He was given a voluntary admission to the Psychiatric Hospital, remained for a short period but subsequently signed himself out.

During this time, the police were actively investigating this crime but were not contacted by the psychiatrist to verify whether in fact this crime had been reported or that the facts as given by Johnson were in fact true. The police continued to investigate this crime with no concrete leads. A series of murders and sexual assaults, extending from 1969 to 1977 took place in which seven (7) females met their death and sexual attacks took place on ten (10) other women. Johnson was subsequently arrested in July, 1977 and charged with the murder of three (3) of these females. He was found not guilty by reason of insanity and is presently in Penetanguishene.

Had the original information on Johnson been made available to the police on a confidential basis, the other crimes may not have been committed. A discreet investigation would have been carried out which in all probability, would have resulted in Johnson's arrest.

Tarasoff v. Regents of the University of California, the decision of the Supreme Court of California mentioned above, arose out of an action brought against University Regents,

psychotherapists employed by the University Hospital and campus police to recover damages for the killing of the plaintiffs' daughter by one Poddar, a psychiatric out-patient at the University Hospital. During therapy, Poddar told his therapist, Dr. Moore, a clinical psychologist, that he intended to kill an unnamed girl, readily identifiable as the plaintiffs' daughter, Tatiana, upon her return from summer vacation. Dr. Moore, with the concurrence of two psychiatrists, decided that Poddar should be committed for observation in a mental hospital, and he notified two campus police officers of his intention. After this oral notification, Dr. Moore sent a letter to the campus Chief of Police requesting police assistance in securing the confinement of Poddar. Poddar was taken into custody by the police, but managed to satisfy them that he was rational and was released on giving his promise to stay away from the intended victim. The director of the Department of Psychiatry at the University Hospital requested the return of Dr. Moore's letter to the campus police chief and directed that the letter and notes that Dr. Moore had taken in therapy be destroyed, and no further action was taken to confine Poddar. Neither the daughter nor her parents, the Tarasoffs, were notified that she was in any danger from Poddar. A few months later, in October, Poddar killed Tatiana Tarasoff.

For our purposes the discussion of this difficult and important case may be simplified by referring only to that part of the plaintiffs' claim that was based upon the defendants' failure to warn of a dangerous patient. In the result the Court held that the circumstances were such as to place the defendants under a duty to warn Tatiana or others likely to inform her of her danger. The negligence in failing to warn and the foreseeability of the risk to the plaintiffs' daughter, along with the resulting damages, established a valid claim.

The duty to warn on the part of the psychotherapists enunciated in the Tarasoff case became the cause of concern and controversy throughout the psychiatric and psychotherapeutic communities in the United States and Canada. Some of the concerns expressed were also referred to in the dissenting judgment of Mr. Justice Clark in the Tarasoff case. They are:

(a) that confidentiality is essential to the effective treatment of the mentally ill, and that imposing a duty on psychotherapists to disclose patient threats to potential victims would greatly impair treatment;

(b) the assurance of confidentiality is essential in order that those requiring a

treatment will not be deterred from seeking assistance and in order to elicit the full disclosure necessary for effective treatment; and

(c) the process of determining potential violence in a patient is inexact and uncertain and the threat of civil liability may lead to overcommitment of patients by psychiatrists.

The following quotations from the majority judgment of Mr. Justice Tobriner in the Tarasoff case indicate the policy considerations to be weighed in balancing the need for patient confidentiality with the protection of society and individuals:

We recognize the difficulty that a therapist encounters in attempting to forecast whether a patient presents a serious danger of violence. Obviously we do not require that the therapist, in making that determination, render a perfect performance: the therapist need only exercise "that reasonable degree of skill, knowledge, and care ordinarily possessed and exercised by members of [that professional specialty] under similar circumstances." Within the broad range of reasonable practice and treatment in which professional opinion and judgment may differ, the therapist is free to exercise his or her own best judgment without liability; proof, aided by hindsight, that he or she judged wrongly is insufficient to establish negligence.

In the instant case, however, the pleadings do not raise any question as to failure of defendant therapists to predict that Poddar presented a serious danger of violence. On the contrary, the present complaints allege that defendant therapists did in fact predict that Poddar would kill, but were negligent in failing to warn.

. . . . .

While the discharge of this duty of due care will necessarily vary with the facts of each case, in each instance the adequacy of the

therapist's conduct must be measured against the traditional negligence standard of the rendition of reasonable care under the circumstances.

. . . . .

We recognize the public interest in supporting effective treatment of mental illness and in protecting the rights of patients to privacy, and the consequent public importance of safeguarding the confidential character of psychotherapeutic communication. Against this interest, however, we must weigh the public interest in safety from violent assault. The Legislature has undertaken the difficult task of balancing the countervailing concerns. In Evidence Code section 1014, it established a broad rule of privilege to protect confidential communications between patient and psychotherapist. In Evidence Code section 1024, however, the Legislature created a specific and limited exception to the psychotherapist-patient privilege:

There is no privilege...if the psychotherapist has reasonable cause to believe that the patient is in such mental or emotional condition as to be dangerous to himself or to the person or property of another and that disclosure of the communication is necessary to prevent the threatened danger.

We realize that the open and confidential character of psychotherapeutic dialogue encourages patients to express threats of violence, few of which are ever executed. Certainly, a therapist should not be encouraged routinely to reveal such threats: such disclosures could seriously disrupt the patient's relationship with his therapist and with the persons threatened. To the contrary, the therapist's obligations to his patient require that he not disclose a confidence unless such disclosure is necessary to avert danger to others, and even



then that he do so discreetly, and in a fashion that would preserve the privacy of his patient to the fullest extent compatible with the prevention of the threatened danger.

The revelation of a communication under the above circumstances is not a breach of trust or a violation of professional ethics; as stated in the Principles of Medical Ethics of the American Medical Association (1957), section 9:

A physician may not reveal the confidence entrusted to him in the course of medical attendance...  
unless he is required to do so by law or unless it becomes necessary in order to protect the welfare of the individual or of the community.

We conclude that the public policy favoring protection of the confidential character of patient-psychotherapist communications must yield to the extent to which disclosure is essential to avert danger to others. The protective privilege ends where the public peril begins.

The Tarasoff case raises the possibility of a difficult problem in the Ontario context. It cannot be said with certainty that an Ontario court would decide a case involving identical circumstances in a different way. It is not entirely clear, in other words, that our courts would refuse to acknowledge the existence of a duty to warn in the very same circumstances. It will be recalled that, for the purpose of professional discipline, it is not professional misconduct for a physician to give information concerning a patient's condition to a person other than the patient if he or she is required to do so by law. If the Tarasoff case is good law in Ontario, that is to say, if it should turn out that the judgment correctly reflects the state of the law in this province, it can be said that, in the circumstances that prevailed in that case, a physician is under a duty, and a legal duty at that, to warn the intended victim of the patient's potential violence. The warning may, to put it another way, come within the words of section 26.21 of Regulation 577/75, "unless required to do so by law." Any other conclusion would bring about the anomaly that a physician can be found guilty of professional misconduct for

doing that which, if he or she fails to do, can expose him or her to civil liability, surely an unacceptable state of affairs. Furthermore, it must be admitted that the recommendation I make does not solve the problem and, in fact, may even make it more apparent. Dilemmas, however, are an inherent fact of life in the practice of a profession and no volume of legislation will ever eliminate them.

Another example of the recurring dilemma was illustrated in the submission of Dr. Alan S. Davidson, a practising psychiatrist. Dr. Davidson was alleged to have been guilty of professional misconduct in releasing confidential information about a patient without that patient's consent and without being required by law to do so. The incident in question occurred within the context of joint counselling. What follows is Dr. Davidson's explanation of the problem he faced:

...It was as a result of my experience in courts and in marriage counselling and then being involved and embroiled in matrimonial conflicts that I ran into a series of most unfortunate cases in which it seemed that persons were in imminent danger of serious injury or death. In one of these, I gave information to a spouse, to the wife, because I had every reason to believe that she would be killed within a matter of days or weeks if her beatings continued as alleged.

I should add that there was verification from a specialist in internal medicine that this person had sustained serious injuries which involved trauma and damage to the liver. As you know, liver or spleen injuries can be fatal.

So under those circumstances I was in a dilemma because the woman who sought my assistance in making a plea before the family court was not at that moment represented by counsel. Her legal counsel was away and his colleagues were reluctant to attend family court with her and I had every reason to feel that she was in dire peril and that her spouse if produced before a courtroom would convince the court that he was entirely reliable and trustworthy and not likely to inflict violence.

So in that context, a person who had come to me with her spouse for marriage counselling and then he had angrily discontinued the marriage counselling sessions, so I was left with the wife, and in that context I gave her a handwritten note which I had prepared about two months previous describing what I felt was wrong with both husband and wife, very briefly, a summary of my observations of both of them. I gave her that document plus other documents on visits that she had had with me subsequent to her husband discontinuing marriage counselling. I gave her these documents to take to court, which she never did. They were never used. But the aggrieved husband felt that I had disclosed confidences about him to her, and on that basis I was brought before the College and tried by a tribunal which included a lawyer and a layperson representative. And to my astonishment, they found me guilty of disclosing information contrary to the law.

Now I thought it was my duty as physician to protect life and that I felt that it was my duty as a citizen to advise the authorities if I felt that someone's life was imperilled, and I had lots of experience with this kind of problem before and knew that it was not easy to approach a court and ask for a subpoena to produce information. It was a cumbersome process. I knew that a visit to a Justice of the Peace was an exercise in futility at that time. They were reluctant to enter into these matrimonial disputes. They veered away from involving themselves. And in the city I found that the police were very reluctant to involve themselves in matrimonial disputes and were more likely to wait until somebody was dead before they intervened.

So that was my dilemma and I felt that I was on safe ground in giving this woman information which had been shared with her husband's lawyer previous to that. I assumed that he had given that information to his client.

MR. STROSBURG: Doctor Davidson, when you started joint counselling at that time, did you discuss with the persons who were becoming involved the parameters of disclosure that you intend to make? By that I mean do you say, for example, to the husband and wife when you see them, now this is a matter of joint counselling so that it has to be for me to use my discretion and decide what is going to be told to the other person, or do you say that confidences will be respected? Do you touch on that when you talk to them in the first instance?

DR. DAVIDSON: Yes, I do. I did. I don't do marital counselling now, I've got away from that. But I certainly did explain that I could not be pledged to secrecy by one party in a matrimonial dispute when the two were seeing me, and they would have to trust my good judgment that I would not disclose harmful things, but would have to share some information with their spouse. But I could not be bound to keep this secret and that, and to disclose that. That I couldn't be having one or another party ordering me to keep certain bits of information secret and others open. And that they would have to trust me.

. . . . .

It's the same situation as you encounter with a teenager who comes in and says now don't tell my mom or dad this or that. I used to say to teenagers that they couldn't do that to me, that if they were having a romance that their parents might not approve of, I would certainly keep that secret. But if they were thinking of killing themselves and I felt concerned that I might have to approach the authorities or their parents I felt that I could not give a blanket assurance that everything told me would be secret. That there were always circumstances where one might have to disclose.

Of course, I took that from another area of medicine altogether where society has long

required physicians to disclose communicable diseases, venereal disease, to disclose that a person poses a threat to society by reason of driving incompetence. There are other areas where society has for long required disclosure.

Anyway, this was my approach and most of the people who saw me were quite content to accept my word that I would have their interests at heart and not do anything knowingly to harm them.

A brief account of the decision of the Discipline Committee of The College of Physicians and Surgeons of Ontario with respect to the alleged misconduct is found in the interim report of the College of March, 1979. In the report Dr. Davidson is not identified by name:

This case concerned an allegation of misconduct that arose prior to the effective date of operation of The Health Disciplines Act. The matter had previously been heard by a different panel of the Discipline Committee on identical facts.

That Committee found the Doctor guilty of professional misconduct under The Health Disciplines Act. That conviction was quashed by the Divisional Court of the Supreme Court of Ontario on the basis that the charge should have been brought under The Medical Act. The Doctor was then charged with professional misconduct under The Medical Act and the hearing proceeded on this charge before the current Discipline Committee.

The Doctor was charged with professional misconduct in that it was alleged he had released a confidential report on a patient to another person without the patient's consent and without being required by law to do so.

The Doctor attended the Discipline Committee hearing with his counsel and pleaded not guilty.



After reviewing all the evidence and the submissions made by counsel on behalf of the Doctor and the submissions by counsel on behalf of the College, the Discipline Committee found that the facts of the charge as presented on behalf of the College have been proved in that the Doctor did release a confidential report on his patient to a third person without his patient's consent and without being required by law to do so. However, in light of all the evidence the Discipline Committee considered that in the circumstances of the case it was their opinion that the Doctor was not guilty of misconduct in a professional respect pursuant to Section 34(3)(c) of The Medical Act.

Although there was a finding that the facts of the charge had been established with respect to the releasing of confidential information without consent or without being required by law to do so, the Discipline Committee, in indicating that this was not professional misconduct under the circumstances, did not explain the conclusion at which it had arrived. In the light of the previous discussion of the Tarasoff case, it is a nice question whether it could not be said that Dr. Davidson was under a duty to warn and therefore fell within the words "unless required to do so by law."

Knowledge which a physician may acquire and which he or she is required ethically, and by legislation, to keep confidential, may include information establishing a real threat of violence to an individual or individuals. This type of problem probably occurs more frequently in the practice of psychotherapists because of their special concern with emotional and mental problems. It is clear that in spite of the wording of the ethical standard of confidentiality, situations arise in which many physicians feel an overriding obligation to society, because of their special knowledge, to take action with respect to the information which otherwise ought to be kept confidential. Again, I refer to the brief of the Ontario Medical Association:

#### VOLUNTARY REPORTING BY PHYSICIANS

15. There are some situations where reporting of a patient's condition is not mandatory but is nevertheless warranted. These are cases in which a patient's condition gives the physician reasonable ground to suspect that a crime has been, or is

about to be, committed, or that the public safety is in jeopardy. We believe that physicians generally have fulfilled their responsibility in this area and that society can continue to rely on the physician's judgment in such cases.

The acknowledgment that, in the past, physicians have made disclosures in situations in which their conscientious concern for interests other than their patients' is another reflection of the eternal dilemma to which I have referred and of the unsatisfactory nature of the strict command implicit in the language of section 26.21 of Regulation 577/75. I can, however, see no justification for a recommendation that the reporting of medical information in the case of the commission of crimes or the prediction of possible future crimes should be mandatory. On the other hand, there is ample evidence to justify amending the legislation governing confidentiality to accommodate the societal needs demonstrated by the experience brought to my attention during the inquiry. There is further discussion of this issue in the section of the report dealing with police and law enforcement, where the following recommendation was first stated.

*Recommendation:*

22. *That the relevant regulations under The Health Disciplines Act, 1974 be amended to provide that, where a health-care provider whose profession falls within The Health Disciplines Act, 1974 and who is not working in a health-care facility or under the direction of a physician has reasonable cause to believe that a patient is in such mental or emotional condition as to be dangerous to himself or the person of another or others and that disclosure of information about the patient is necessary to prevent the threatened danger, the health-care provider may disclose such information to the police or others without the consent of the patient. Disclosure made under that reasonable belief shall not amount to professional misconduct.*

As I have indicated, implementing this recommendation will not eliminate dilemmas. The difficult task will remain for the physician to select the form of intervention most consistent

with upholding the rights and the needs of the patient, which, depending on the circumstances, may require taking action to commit, advising the police or other appropriate authorities, contacting the party or parties threatened, or involving an existing social support system to assist in monitoring the patient's behaviour, to mention a few of the options.

## Nurses

Earlier in this discussion I set out the language of the regulations relating to the relationship between breach of confidentiality and professional misconduct for the professions governed by The Health Disciplines Act, 1974. In the case of nurses, Regulation 578/75 contains the following definition of professional misconduct in section 21:

- (k) failure to exercise discretion in respect of the disclosure of confidential information about a patient;

This definition, when compared with those applicable to the other professions, is exceptional. It does not prohibit disclosure of sensitive information about patients; it simply requires the exercise of discretion in the act of disclosure.

During the course of this inquiry, I received considerable assistance from the written and oral submissions of the College of Nurses of Ontario, the Registered Nurses' Association of Ontario, the Association of Nursing Directors and Supervisors of Ontario Official Health Agencies, and other groups and associations representing the various concerns of the nursing profession. One of the many questions I discussed with them was their perception of the effect of a discretionary sharing of information on confidentiality. At our hearings I learned about the background of the language of the definition of professional misconduct, from Joan MacDonald, the director of the College of Nurses of Ontario:

MISS MACDONALD: I think we were thinking about professional judgment and we have that kind of judgment and respect for a patient, and...

MR. COMMISSIONER: So would a physician, surely.

MISS MACDONALD: We must trust our people.

MR. COMMISSIONER: Is that the reason?

MISS MACDONALD: It's probably more comfortable to have a black and white ruling, but it was our counsel's feeling when these were developed that there should be that judgment made.

MR. SHARPE (Assistant Commission Counsel): Does that section, the discretion, apply only to the disclosure to other members of the health care team, or does the discretion include third parties?

MISS MACDONALD: Our interpretation is that it's the health care team.

MR. SHARPE: So there is no discretion in the nurse to decide to disclose confidential information to a police officer, let's say, in the absence of a subpoena?

MISS MACDONALD: That has been the way we have interpreted it.

In a written submission, the Registered Nurses' Association of Ontario described that Association's view of the nurse's discretion with respect to the disclosure of confidential patient information:

The factors considered by the nurse in making a judgment about sharing information are the rights, well-being and safety of the client balanced against the rights, well-being and safety of others and society.

Disclosure of information for such purposes as peer review, disciplinary hearings, quality assurance programs and research must be strictly controlled in such a way as to guarantee confidentiality for the client.

Under some legislation, such as the Child Welfare Act, the nurse is required to report to the appropriate authority certain specific information about a client.

. . . . .

In summary, the registered nurse is obligated by a code of ethics, legislation and standards of nursing practice...to protect the confidentiality of any personal information about the client, however gained. Only that information necessary in planning and implementing the client's care is shared and then only with those members of the health care team directly involved with that care. The nurse is required to use judgment in determining under what conditions information will be shared and with whom.

The registered nurse, committed to promoting the well-being of man and protecting the dignity, worth and autonomy of each person, believes that a client has a right to expect that information shared in the process of care will be considered as confidential and treated with discretion.

As an autonomous individual, a client has the right to refuse to a member of the health team permission to share information. The role of the nurse is to ensure that he/she fully understands the consequences of such a decision.

The absence of a prohibition of disclosure of confidential information must make it difficult for the Discipline Committee of the College of Nurses to impose a penalty when there has been an impugned disclosure of confidential information. No assistance is given the nurse to enable him or her to determine under what circumstances the disclosure of information would be considered a proper exercise of discretion. This concern was expressed at our hearings by Jocelyn Hezekiah of the Registered Nurses' Association of Ontario:

On most occasions the priorities are clear when the individual's and society's interest come into competition. There are occasions when the determination of the priority of competing interests is left to the judgment of the health professional, as in the case of a threat to a third party or to society, with no specific guidance available in legislation or the ethical code.



## Recommendation:

80. That the definition of professional misconduct applicable to all health-care providers whose professions fall within The Health Disciplines Act, 1974 reflect the basic requirement that patient information, including information with respect to professional services performed, should be kept confidential, and not disclosed to any other person without the consent of the patient, unless required by law, or unless there is a threat to the life or safety of the patient or another.

The sharing of health information by nurses with other members of the health-care team is another difficult issue. The questions of the transfer of health information between hospitals and other health facilities, the release of information by public health units from pupil health records and the handling of occupational health information are dealt with elsewhere in this report.

## Pharmacists

In that part of the report that deals with the information gathering practices of the private investigation firm of Jolie and Todd in Windsor, a description is given of the records kept by pharmacists and their obligations with respect to confidentiality. During our policy hearings, I had the benefit of very thoughtful and detailed submissions from the Ontario College of Pharmacists and from representatives of Green Shield Prepaid Services Inc., a private plan for the provision of prepaid pharmaceutical and other services.

The Health Disciplines Act, 1974 does not impose an obligation of confidentiality upon practising pharmacists. Regulation 579/75 under that Act contains the following definition of professional misconduct in section 47:

- (x) conduct or an act relevant to the practice of a pharmacist that, having regard to all the circumstances, would reasonably be regarded by members as disgraceful, dishonourable or unprofessional.

I have no doubt that pharmacists and the Ontario College of Pharmacists consider prescription records to be confidential. The Code of Ethics, first adopted by the College in 1969, provides as follows:

#### Section 6

A pharmacist should respect the confidential and personal nature of his professional record; except where the best interest of the patient requires or the law demands, he should not disclose such information to anyone without proper patient authorization.

In the explanatory material which accompanied the Code of Ethics when it was distributed to members the following statement appeared:

Section 6 recognizes that a pharmacist may ethically disclose information from his patient and prescription records where it is in the best interests of the patient. He should disclose information when it is required by law or when it is properly authorized by the patient. He may also release information for legitimate research purposes, where the obligation of confidentiality to the patient is not compromised.

It seems to me to be an inescapable inference that a breach of the Code of Ethics relating to the obligation would reasonably be regarded by pharmacists as disgraceful, dishonourable or unprofessional, and would be considered professional misconduct. It is my view that what is implicit in the legislative scheme should be made express. Implementation of recommendation 80 would have this effect.

One of the major concerns expressed by both Green Shield Prepaid Services Inc. and the Ontario College of Pharmacists related to the impact of electronic data processing on pharmacists' patient records, previously kept on manual prescription files in individual pharmacies and currently being stored to an increasingly greater degree in centralized computers. One of the main factors leading to the computerization of the pharmacists' records is the expansion of third party payment programmes, both of the private variety, as represented by Green Shield Prepaid Services Inc., and government programmes, such as the Ontario Drug Benefit programme administered by the Ministry of Health.

This awareness of the volume of information identifying patients, along with drug prescriptions and other personal details, and of the potential for providing a variety of different reports creating a patient drug profile, is reflected in the following remarks taken from the brief of the Ontario College of Pharmacists:

#### PRESCRIPTION RECORDS ON COMPUTERS

There are two aspects to this matter. The first is in connection with the information that has been collected by third-party payors and stored in their computers and the second is the advent of computers in pharmacy practice.

As far as the former is concerned, the information gathered and stored in the computer of a third-party payor would be the same as that to be found on the prescription files of a particular pharmacy but it would be compiled and arranged in a different way. Therefore, such information is useful in an investigation involving a pharmacist and claims made to the third-party payor. There would be no legal barrier to obtaining such information in our view, and the third-party payor is likely to want to cooperate in any investigation by the College involving a pharmacist.

In the past few years, the use of computers by pharmacists in their dispensaries has become popular. In October, 1973 the following notice appeared in the College Newsletter:

#### Computerized Prescription Records

It has been drawn to the attention of the College that some pharmacists have been approached with respect to computerized prescription records. There are a number of unanswered questions with respect to legal matters and confidentiality in connection with the computerization of prescription records. The College is studying this question and registrants are advised to use

discretion before signing contracts binding them to a computerized prescription record system.

In June, 1975, a notice was sent to all pharmacists regarding the use of computers in prescription records and the following statement was included with respect to confidentiality:

Prescription records must be kept confidential. This limits access to such records to the patient concerned, or the patient's designated agent, the physician concerned and the pharmacist.

Various commercial enterprises have introduced computerized systems for pharmacies and the College has attempted to advise these providers of the service as well as the pharmacist. With respect to "on line" computers the College has insisted on so called "dedicated lines" and the principle that one pharmacy not be able to access information on a person's drug history for another pharmacy, including other pharmacies that might be associated with the same chain of pharmacies. This raises an interesting question as to confidentiality on one hand and the benefit to the patient of sharing drug interaction and other information on the other. To date, we have opted for preserving confidentiality.

At the present time, the College has no authority to approve computerized systems, and there are no legal standards with respect to such computers as far as their use in pharmacy is concerned. It is the pharmacist's responsibility to comply with the laws and ethics of his profession and he should not become involved with a computerized system that does not permit him to comply with such laws and ethics. The College has, so far, received good cooperation from the providers of computer systems who have followed our suggestions with respect to confidentiality and other matters.

Consideration should, however, be given to the need for investigation and/or legislation which would ensure the preservation of confidentiality of information maintained by central processors facilities. This would include the disposition of a particular client's information if the client wishes to terminate an association with a computer company. The private nature of computer data on individuals has given rise to legislation in the United States which requires terminal operators to access information on the basis of specific need only. (The Federal Computer Systems Protection Act S.B. 1766).

My views of desirable minimum standards for security of information stored in computers are given elsewhere in this report. The pharmacist, as a health-care provider required to maintain standards of confidentiality with respect to patient information, must be expected to require adherence to those standards by his or her employees. He or she must also acquire a knowledge and understanding of, and assurance of compliance with, these standards of confidentiality from computer facilities and service bureaus to whom he or she entrusts patient information for processing and storage. This obligation is recognized in the brief of the Ontario College of Pharmacists.

With respect to patient information which has been collected by third-party payers, there is no reason why a patient who is required to provide information should not be entitled to the assurance that the information given for insurance payment purposes will be treated with the same concern for confidentiality that he or she expects from the original health-care provider.

## Health Service Organizations

Health service organizations provide a relatively new method of delivering primary health care to patients in Ontario on a basis other than fee for service. During the course of our hearings, several physicians participating in two of these organizations expressed concern over certain aspects of the operation of HSOs as they affected confidentiality of patient records. The evidence and submissions at our hearings about HSOs related to our examination of the Lawrence Heights Medical Centre and the Lakeshore Area Multi-Services Project Inc. However, the discussion and recommendations that follow have



application to the confidentiality of health information in HSOs generally.

In a letter to Commission Counsel dated June 23, 1978, W. Alan Backley, then Deputy Minister of Health, provided the following information about health service organizations operating in Ontario at that time:

1. There are thirty (30) Health Service Organizations (HSOs) in the Province of Ontario of which the Lawrence Heights Medical Centre is one. These organizations are not identical in auspices, operation or administration.
2. Fourteen (14) of the HSOs, including the Lawrence Heights Medical Centre, are operated by Boards of Directors comprised of citizens in the community. Ten (10) other HSOs are operated by physicians; three (3) are family medical practice teaching units operated by universities; the remaining three (3) are operated by a Board of Trade, municipality or insurance co-operative.
3. There is a contract in existence between the Centre and the Ministry of Health, a copy of which is enclosed. The Agreement is basically (to use the wording of section 6(1)(d) of The Ministry of Health Act, 1972),

for the provision of health services...and for the payment of remuneration for such health services on a basis other than fee for service.

. . . . .

6. There is no provision for Ministry of Health approval of the by-laws of the Centre.
7. The Ministry has not made any express provision for control over access, by members of the Board, to the medical records of the Centre. It is thought

that there will be occasions when the Board, as the provider of health services, has a valid interest in the contents of the medical record of a patient of the Centre, and it was not anticipated that access might be sought by a Board member for any improper purpose.

Raymond Grant Berry, the Director of the Program Development Branch of the Community Health Division of the Ministry, gave the following evidence at our hearings:

As far as the ministry is concerned, it has been an attempt to respond to requests from groups of citizens to provide themselves with a different organization's services. In some cases it has been a recognition of the needs for service in an area where none existed. In some northern communities, for example. In which case the HSO concept is very much like other programs which we are, currently have in place in some of those communities. In some cases it was to meet the request for provision of services as a health organization which are not currently provided under OHIP payment, such as nurse/practitioners or nutritionists or whatever.

Now the only, I shouldn't say that. There are a number of things that the ministry felt were essential to assure itself about and that was that the services which would be provided would be at least equivalent and that they would have a degree of comprehensiveness about them which is not necessarily required in the current health system. That is that there would be services provided twenty-four hours a day and so on. Now, this led, of course, to a wide variation in the membership, in the size and in the organization. The contracts which we have used, of which you have two examples, do differ from each other in some cases on the basis of a fair amount of detail about the kind of information which we would like to have.

I think we want to be assured that the services which are provided are at least equivalent. But we wish in addition to that to have the opportunity of studying these activities and these organizations to attempt to identify those elements of programs which might be put together in an expansion of the program in future.

It is not our intention to govern the practice of medicine within the HSOs and we have requested, I am not entirely sure that each contract requires that there be a contract between the physician and the agency, but that certainly is our intent that the contractual agreement about the way in which services would be provided would be a subject for discussion and decision by the HSO, if it is a community board, and the physicians.

The following sections from the agreement entered into between the Ministry of Health and one of the health service organizations gave rise to concerns about government access to patient records:

3. (1) The Centre agrees that any persons designated by the Minister after consultation with the Centre may conduct a study of quality of care and patient attitude relating to the Centre, and that patient anonymity and confidentiality of medical records shall be maintained.

(2) The Centre agrees to give to any such persons designated,

- (a) free access to the Centre, its patients and its records;
- (b) generally such other privileges and information as may reasonably be required to effectively conduct the study.

. . . . .

6. (1) The Centre will make and keep complete patient records of each patient visit to the Centre.

(2) A copy of such records shall remain at the Centre in some form.

7. During and after the term of this Agreement, the Centre will allow any official of the Audit Services Branch of the Ministry of Health or any other person appointed by the Minister, free access at all times to all books of account, bank accounts, vouchers, and any documents and correspondence relating to financial transactions undertaken by the Centre which relate to this Agreement.

Mr. Berry outlined the position of the Ministry on its possible needs for access to patient information in the supervision of health service organizations:

...We have two items, two issues. One is concerned with accounting procedures. That is, just the handling of money. The other has to do with the actual quality of care which is provided. You must recognize that changing the system, which is I think a pretty good system we have in Ontario, can only be done with some degree of caution, and our approach to that has been one in which we would specify that we would have the opportunity of examining and studying quality of care which is provided under this new system, and that is included I think in almost all of the contracts. It may not actually be in all of the contracts, but it certainly is in the ones we have there.

Now it raises some important detail issues which we have not addressed, and that is how this might actually be done. Certainly we would not, I can't think of any circumstance in which we would carry out a quality care study, unless there was a complaint made with regard to an HSO, unless the quality of care study was being carried out with the agreement of all those who were participants. What I am saying is that in one case

is that if there were complaints laid at the door of an HSO about the quality of care, then I think we would exercise considerably more authority in that situation than just the study to identify whether the system was working.

MISS SMITH (Associate Commission Counsel): Would you take the position then that this provision in the agreement would allow you to enter a centre and to look at patient records?

A. I would think it probably does. How we would actually do that, I think would have to be studied. In the case in which quality of study has been conducted in HSOs, that has been conducted by people, physicians who are acceptable to the people in the HSO, although the contract doesn't specify that. I expect that's how we would operate. I think the contract does give us that permission.

To the extent that financial audit and professional monitoring by the Ministry of Health are necessary and authorized by the terms of the agreements and the provisions for audit contained in The Health Insurance Act, 1972, the recommendations made earlier with respect to audit and professional monitoring are applicable.

One agreement between an HSO and its physicians contains this provision with respect to the ownership of medical records:

14. Upon the termination of this Agreement the Doctor shall have no right, title or interest in any medical practice, assets or records of LAMP except in respect of the medical information contained in LAMP records respecting any patient who in writing directs LAMP to provide such information to the doctor.

Dr. Trevor Hancock, a physician who worked for two years with a health service organization as a family physician, took the following position in his brief:

Community sponsored HSOs face a further unique problem, which is that the medical records are in fact owned by the Community



Board. It must be very categorically stated that under no circumstances does ownership of these records imply access to the records except by the medical staff or those authorized by them or the patient to have access.

Members of the boards of the two health service organizations who appeared at our hearings said that it was not their position that they should have access to the patients' records. However, the agreement to which I have referred does support an argument that the records are to be kept and maintained by the board of the health service organization. If the argument is valid, it creates the possibility of a conflict between the physician's ethical obligation to keep the medical records confidential and the access by non-medical staff and board members. In fact, Mr. Backley's letter outlining the structure of health service organizations expressly refers to the possibility that there might be access to those records by members of the board. It should be remembered that the nature of a health service organization is such that board members very likely know many of the centre's patients personally. I am not persuaded that they need the right of access to the organization's patients' records.

The position of one of these such multi-service organizations was put in the brief of Joseph P. Leonard, executive director of the Lakeshore Area Multi-Services Project Inc.:

All members of the LAMP team, both direct service and administrative staff are fully aware of the ethical obligations entailed in the professional delivery of health and social services. These obligations place limits on the nature of information which may be sought as well as restrictions on the use to which it may be put. Confidentiality thus contributes to a clarification of the function of LAMP and to the development of professional self discipline. It also places an obligation on the client to provide helpful information as well as safeguarding his/her right to control the use and disclosure of such information.

LAMP's obligation for confidentiality extends to all aspects of administration, for application or inquiry, throughout the continuing relationship and after the client has ceased to receive services. This obligation is binding on individual workers, on

all LAMP personnel as well as on the organization as a corporate entity. It applies equally to all records - medical and social service. Thus as in the case of hospitals, although the administration and care of medical records is the direct responsibility of the medical staff, ownership of the records belongs to LAMP Inc., which holds ultimate responsibility for policy and administration. The LAMP Board has no direct access to these files.

LAMP represents one of many demonstration projects whose goal is to provide co-ordinated services to their local communities. It has long been recognized that fragmented, specialized services are costly and inefficient in meeting the needs of multi-problem families. Innovations in the field of human services delivery face many problems, particularly in overcoming traditional concepts and rigidities in some agency mandates.

In this submission, no argument is made for the necessity for access to records on the part of the board members of the organization.

*Recommendation:*

*81. That agreements between the Ministry of Health and Health Service Organizations provide:*

- (a) that ownership and control of patients' medical records by the board of the Health Service Organization carry with it an obligation on the part of the board to maintain the confidentiality of the medical records;*
- (b) that there be no access by the Health Service Organization's board or its members and the staff, other than the professional staff, to the patients' medical records without the consent of the patients; and*

*(c) that the board of the Health Service Organization not permit the disclosure of medical information from the medical records of a patient without the consent of the patient unless required by law or except where there exists a threat to the life or safety of the patient or another.*

## Psychologists

The Ontario Board of Examiners in Psychology submitted a brief and made oral submissions which emphasized the predicament of employed psychologists and, in particular, psychologists employed by school boards. A discussion of these issues appears in my treatment of school health records.

Clinical psychologists are professional health-care providers. No distinction should be made between the health information generated in the course of providing psychological services and health information pertaining to physical health. Psychologists should be under the same obligation of confidentiality in respect of their clients' records as other health-care providers and should be subject to the same exceptions.

## Access to One's Own Health Information

As I pointed out in the introduction to this report, patient access was one of the most controversial and emotional subjects dealt with in our inquiry. Current Ontario legislation does not recognize the right of a patient to access to his or her health information. No remedy exists to which the patient can resort if he or she is refused access.

In the context of the subject of health information, Ontario society, I believe, is not significantly different from the rest of North American society, in which there is a discernible trend toward an individual's right of access to personal information about himself or herself, including his or her own health information. In the language of Professor Alan F. Westin, in "Medical Records: Should Patients Have Access?" in Hastings Center Report 7:6 (December 1977) at page 23:

The movement to give patients a legal right of access to their medical records parallels attempts by parents and students to get access to school records, and of consumers to get access to credit bureau records. These are part of a growing citizens' movement to affirm individual self-determination and place limits on the power of institutions to determine important aspects of people's lives without due-process-oriented procedures.

This movement is quite evident in jurisdictions in the United States and Canada. In the U.S.A., a bill "To protect the privacy of medical information maintained by medical care facilities" (the Federal Privacy of Medical Information Act), now before the House of Representatives, defines the rights of patients. Section 111(a)(1) of the bill says,

Except as provided under subsection (b), a medical care facility shall permit a patient to inspect any medical information that the facility maintains about the patient, and shall permit the patient to have a copy of

the information. The patient may designate in writing another individual to inspect, or to have a copy of, the information on behalf of the patient or to accompany the patient during the inspection. When a patient or other individual inspects or obtains a copy of medical information under this subsection, the facility may offer to explain or interpret the information.

Although the list of exceptions under subsection (b) is extensive, the rule is clear. As a matter of principle, however, there is one feature of the bill which I cannot endorse. Subsections (b)(2) and (b)(3) provide as follows:

(2) If information is withheld under paragraph (1)(A), the facility shall permit the information to be inspected and copied by a person, selected by the patient, who is (A) a licensed or certified health professional, (B) an attorney, (C) a family member, or (D) other person permitted to be designated under State law. If inspection or copying of medical information by the family member selected by the patient would cause sufficient harm to the patient or to a family member so as to outweigh the desirability of permitting access, the facility is not required to permit access by the family member, but the facility shall permit the patient to select another person in accordance with this paragraph.

I confess that I have great difficulty with the concept that a patient's right to see personal information about himself or herself can be satisfied by denying the patient access to the information but giving it to his or her representative. I concede that there is no objection to this course of action if the patient agrees to it. But where he or she insists on access, I cannot understand why it is a satisfactory compromise to give the information to the patient's agent. I should have thought that if an agent was entitled to information, so was his or her principal.

The introduction of the U.S. bill was preceded by the hearings of the Privacy Protection Study Commission which, in July, 1977, submitted its persuasive and influential report, Personal Privacy in an Information Society. The report points out that nine states then granted a patient "the right to



inspect and, in some instances, obtain copies of his medical records," and then goes on to make the following recommendation at page 298:

That upon request, an individual who is the subject of a medical record maintained by a medical-care provider, or another responsible person designated by the individual, be allowed to have access to that medical record, including an opportunity to see and copy it. The medical-care provider should be able to charge a reasonable fee (not to exceed the amount charged to third parties) for preparing and copying the record.

Ontario itself has not escaped the movement. In 1978, The Mental Health Act, R.S.O. 1970, chapter 269, was amended by the enactment of section 26a in The Mental Health Amendment Act, 1978, S.O. 1978, chapter 50, section 10. Subsection 3 of section 26a reads, in part, as follows:

The officer in charge and the attending physician in the psychiatric facility in which a clinical record was prepared may examine the clinical record and the officer in charge may disclose or transmit the clinical record to or permit the examination of the clinical record by,

- (a) where the patient has attained the age of majority and is mentally competent, any person with the consent of the patient;

For the purpose of this discussion I shall assume that the words "any person" in that subsection include the patient himself or herself. It will be observed that the provision just quoted does not confer an unrestricted right of access. The matter is entrusted to the discretion of the officer in charge of the psychiatric facility. This state of affairs was the subject of comment in the recent (1979) report of the Legal Task Force of the Committee on Mental Health Services in Ontario. At page 22 of the report the following statement is found:

We have received no substantial criticism of the right of the patient to receive his psychiatric record unless his physician decides that it would do him harm to have access. In fact we feel that s.26a is an excellent

improvement in the law, and note that it accords with the approach to medical records used in federal legislation.

→ The section 26a(3) is drafted in permissive language, however: "the officer in charge may disclose..." It would be preferable if the statute clearly spelled out the officer in charge shall disclose unless such disclosure is not in the best interests of the patient. (This style has in fact been used in subsections (5) to (9)).

Elsewhere in Canada, three provinces, Alberta, Quebec and Nova Scotia, give the patient a statutory right of access to his or her hospital records. In Alberta, section 35(3) of The Alberta Hospitals Act, R.S.A. 1970, chapter 174, as amended, and section 50.1(4) of The Mental Health Act, 1972, S.A. 1972, chapter 118, as amended, provide that information obtained from the records is confidential. Under The Alberta Hospitals Act, the right of access is defined in subsections 5 to 8 of section 35. The relevant provisions of these subsections read as follows:

35. (5) Notwithstanding subsection (3) [the general confidentiality subsection] or any other law, a board or employee of a board, the Minister or person authorized by the Minister, or a physician may

(a) with the written consent of a patient divulge any diagnoses, record or information relating to the patient to any person

. . . . .

(6) Notwithstanding subsection (3) or any other law, where a board, an employee of the board, the Minister, or a person authorized by the Minister, or a physician

(a) is unable to divulge any diagnoses, record or information relating to a patient by reason of subsection (3), or

(b) refuses to divulge any diagnoses, record or information relating to a patient pursuant to subsection (5),

the patient or his legal representative may apply to the court for an order directing the person having such diagnoses, records or information to release them or a copy of them to the patient or his legal representative or to such other person named in the order.

(7) An application under subsection (6) shall be made

. . . . .

(b) by way of originating notice of motion to the Supreme Court of Alberta or a district court...

(8) An application under subsection (6) shall be heard in camera and on the hearing of the motion the onus of showing why the order should not be made for the release of the diagnoses, records or information, or a copy thereof, is on the respondent to the motion.

A similar right of access is granted to mental health patients in section 50.1 of The Mental Health Act, 1972. The Alberta Hospitals Act and The Mental Health Act, 1972 apply to records in public and private hospitals, and in nursing homes.

In Quebec, the relevant provisions of section 7 of the Health and Social Services Act, S.Q. 1971, chapter 48, as amended, are as follows:

The medical records of the recipients [of health or social services] in an establishment [a local community service centre, a hospital centre, a functional rehabilitation centre, a social service centre or a reception centre] shall be confidential. No person shall give or take verbal or written communication of them or otherwise have access to them...except with the express or implied consent of the recipient...

A recipient to whom an establishment refuses access to his record or refuses to give written or verbal communication of it may, on summary motion, apply to a judge of the

Superior Court, Provincial Court, Court of the Sessions or Youth Court or to the Commission, to obtain access to or communication of it, as the case may be.

The judge shall order such establishment to give such recipient access to his record, or communication of it, as the case may be, unless he is of opinion that it would be seriously prejudicial to the health of such recipient to examine his record.

The new Medical Code of Ethics, which became effective in April, 1980, contains this provision:

4.02 Sauf quand cela est préjudiciable à la santé du patient, le médecin doit respecter le droit de ce patient de prendre connaissance des documents qui le concernent dans tout dossier constitué à son sujet et d'obtenir une copie de ces documents.

Under this provision, a physician must respect the right of his or her patient to know the contents of documents relating to him or her in any file maintained for him or her and to obtain a copy of these documents.

The corresponding legislation in Nova Scotia is the Hospitals Act, R.S.N.S. 1967, chapter 249, as amended. The relevant provisions are found in the following subsections of section 63:

(1) The records and particulars of a hospital concerning a person or patient in the hospital or a person or patient formerly in the hospital shall be confidential and shall not be made available to any person or agency except with the consent or authorization of the person or patient concerned.

. . . . .

(3) Notwithstanding subsections (1) and (2), a hospital or qualified medical practitioner may refuse to make available information from the records or particulars of a person or patient if he has reasonable grounds to believe it would not be in the

best interest of the patient to make available that information.

(4) If a hospital or a qualified medical practitioner refuses to make available the records and particulars of a person upon request by that person or upon authorization of that person or agency...then the person requesting the records and particulars or authorized to receive the same may make application to a county court judge and such judge shall in his discretion determine whether the records and particulars shall be made available and to what extent.

These provincial statutes cannot solve all the problems that arise with regard to access to one's own health information but do, I am sure, solve a great many of them. Moreover, by establishing that the general rule is one of access, and by creating a mechanism by which a refusal to give access may be impartially and objectively examined, they have an important prophylactic effect. They make it more likely that hospitals and physicians will not refuse disclosure out of traditional paternalistic habits of thought but will do so only in cases in which they sincerely believe that it would be harmful to patients to see their records. These cases are, I am sure, a good deal rarer than is generally believed among physicians, according to the available evidence.

At my request, and in its customary spirit of co-operation, the Ontario Medical Association communicated with the Alberta Medical Association to inquire into their members' experience with the Alberta legislation. On behalf of the Ontario Medical Association, Dr. J.A. Saunders, Director of Health Services, reported to me the results of the inquiry made and the concern of the Association:

The Ontario Medical Association has received a reply from the Alberta Medical Association responding to our inquiries into those areas of the Alberta Public Hospitals Act which were identified during our meeting with you.

The A.M.A. states that, as far as they are aware, Subsections 6, 7, and 8 of Section 35 of the Alberta Public Hospitals Act were utilized periodically. There are no statistics to enumerate how often patients have



resorted to these sections, but certainly not frequently.

Apparently, the Alberta Medical Association does not have any major misgivings about the legislation, although there is a feeling amongst the physicians of the Hospital Committee of that Association that patient access to the medical record may make the record less effective. There is no evidence, nor is there likely to be, that full information is not recorded, but some physicians in private admit that confidential information is retained in their own private records rather than placed on the hospital record.

This is, of course, our fear. Legislation allowing full disclosure of a physician's record may affect the completeness of the information placed in the medical record. The possibility of full disclosure may also affect the consultant's willingness to be complete and candid in communicating with other attending physicians which ultimately could affect the care that is provided to the patient.

Having stated our concerns, which we believe are very real, we recognize that there may be a need to allow patients to have some access to information that is contained in their medical records. If indeed there is to be patient access to medical records, then we would like to suggest a mechanism similar to the mechanism in effect in Alberta.

As there are times when full revelation of a medical record could cause a negative outcome during the course of a patient's treatment, a method of evaluating whether it is advisable to release some or all of the information in a medical record should be established, and the responsibility for making decisions, where there is controversy, be vested in an independent body such as the court.

The process of evaluating the advisability of release of information from medical records should allow for the fair presentation of argument, the establishment of criteria for assessment and an impartial judgment, if patient access to medical records is established.

In its earlier brief, the Ontario Medical Association had submitted that I should make this recommendation:

That the laws of Ontario recognize a patient's right to information from his medical record, but require that access to such record be only through his attending physician or another physician with responsibility for the patient's care.

The Ontario Medical Association was only one of many bodies and individuals to make submissions about patient access. In fact, approximately one out of every four written submissions made during the inquiry had something to say about the subject and a large proportion of the policy hearings was devoted to it. Few of those who appeared at the hearings were content with the current state of the law in Ontario. In addition to The Mental Health Act, to which reference has already been made, there are three regulations that have some relationship with the question. The first is Regulation 729, the "Hospital Management" regulation, made under The Public Hospitals Act, R.S.O. 1970, chapter 378, the second is Regulation 196/72, made under The Nursing Homes Act, 1972, S.O. 1972, chapter 11, and the third is Regulation 557/75, made under The Health Disciplines Act, 1974, S.O. 1974, chapter 47. The first two, of course, are concerned with institutions, and the third with physicians. The relevant portion of subsection 5 of section 48 of Regulation 729 says this:

A board [of a public hospital] may permit,

. . . . .

(c) a person who presents a written request signed by,

(i) the patient,

(ii) where the record is of a former patient, deceased, his personal representative; or

(iii) the parent or guardian of an unmarried patient under eighteen years of age;

. . . . .

to inspect and receive information from a medical record and to be given copies therefrom.

My interpretation of this provision is that a "person" who may be given permission by a board to inspect his or her medical record includes the patient himself or herself and is not confined to third persons who may be permitted by the board to see the record upon the production of the patient's signed, written request. It will be observed that the language is permissive. The board may give the necessary permission. Of course, the board may also refuse permission, in which event no remedy is given to the patient enabling him or her to challenge the refusal. One reported judgment suggested otherwise and required a hospital, against which no action had been brought, to disclose to a mother, the personal representative, her deceased daughter's medical record. In Strazdins v. Orthopaedic & Arthritic Hospital Toronto (1978), 22 O.R. (2d) 47, Mr. Justice Eberle held that the hospital's reason for refusing to release the record--that to do so would facilitate the initiation of unfounded litigation--was not a sufficient reason for refusing to give the applicant a copy of the record and ordered that it do so. More recently, however, in a very similar case it was held that a court had no authority to compel a hospital to release a medical record to the personal representative of a deceased former patient in the light of the permissive language of section 48(5) of Regulation 729. In unambiguous language, however, the Court expressed the opinion that, although the hospital could not be compelled to release the record, the patient or the patient's personal representative had such an important interest in the contents of the record that, as a matter of principle, the hospital ought to do so. In Re Mitchell and St. Michael's Hospital (Supreme Court of Ontario, June 6, 1980) Mr. Justice Maloney explained his decision as follows, at pages 6-7 of his reasons for judgment:

...I wish to make it very clear that I have no hesitation in expressing the view that the respondent hospital should release the hospital records to the applicant and allow him to take copies therefrom, providing that he submits a proper written request to the hospital. The applicant is the personal

representative of the deceased patient and the provisions of s. 48(5)(c) of Regulation 729 of The Public Hospitals Act provide that the hospital may permit the patient or, when deceased, the personal representative, to inspect and receive information from a medical record upon a proper written application being made to the hospital. Furthermore, I agree with my brother Eberle that it is illogical to require that someone first must start an action in order to be entitled to come before the courts to get production of hospital records. However, I cannot agree with my brother Eberle, or my brother Carruthers, that under the authority of Rule 611 or s. 48 of Regulation 729 I have the jurisdiction to order the release of the hospital records...

Furthermore, s. 11 of the Act provides that hospital records are the property of the hospital and s. 48(5) provides only that the Board may permit certain persons, including the personal representative, to inspect or have copies of the medical records. The wording of the section is permissive, not mandatory, and unfortunately the section does not provide for any procedure, either in the courts or otherwise, whereby production can be compelled or a refusal reviewed.

He concluded his judgment with the following language, at page 8:

Nevertheless, for all the reasons stated above I conclude that I must reluctantly dismiss the application. It is well established that the jurisdiction of the court on an originating motion is confined to that which is specifically conferred by statute or the rules and in this case the jurisdiction to proceed on an originating motion is conferred neither by statute nor the rules. However, while I am not prepared to make an order for the production and inspection of the medical records, I repeat that I am strongly of the view that production and inspection of the medical records should be made to the application upon proper written

application being made to the hospital. As set out in s. 48(5) of Regulation 729, the legislature has made provision for the release of copies of medical records and where, as is the case here, the party applying for the records comes within those provisions of s. 48(5), the hospital should not require the intervention of the courts before releasing the records to persons with such an obvious and legitimate interest in them.

Most apposite to this discussion is the following expression of opinion, at pages 7-8 of his reasons:

By virtue of s. 11 of the Act, medical records are "the property of the hospital and shall be kept in the custody of the administrator", but it seems to me that a patient or the personal representative of a deceased patient, has something akin to a proprietary interest in the contents of those records and s. 11 should in no way operate to prevent appropriate inspection or provision of copies. [emphasis added]

That which Mr. Justice Maloney held he had no power to compel ought, by appropriate legislation, to be made the right of patients or their personal representatives, subject to appropriate safeguards or exceptions to protect the interests of patients and third parties.

Subsection 4 of section 91 of Regulation 196/72 made under The Nursing Homes Act, 1972 provides as follows:

Notwithstanding subsection 1, [which provides that, subject to subsections 2, 3 and 4, no person other than an inspector shall have access to the medical or drug record of a resident]

. . . . .

(d) a person who presents a written request signed by,

(i) the resident,



(ii) where the record is of a former resident now deceased, his personal representative, or

(iii) the parent or guardian of an unmarried resident under eighteen years of age,

may be permitted to inspect and receive information from the resident's medical or drug record and be given copies therefrom.

Regulation 577/75, made under the authority of The Health Disciplines Act, 1974, contains, in paragraph 26 of section 26, this definition of "professional misconduct":

failing to provide within a reasonable time and without cause any report or certificate requested by a patient or his authorized agent in respect of an examination or treatment performed by the member; [of The College of Physicians and Surgeons of Ontario];

The intention reflected by the language of this definition is not clear. The kind of information covered by the words "report or certificate" is uncertain. Whatever the definition means, it certainly does not purport to give the patient a right of access to his or her very record created or maintained by the physician.

Spokesmen for public interest groups who appeared at our hearings supported the patient's right of access to his or her medical record. The Patients' Rights Association submitted "that patients be given an explicit legal right to see, copy and obtain corrections to their own health record." The Canadian Civil Liberties Association said that,

What is needed is a clear statutory enshrinement of the principle that the effective control of patient information must reside in the patient affected. In practice, this would mean that, presumptively at least, two consequences would follow:

1. Patients would have a right of direct access to their own records.

2. Those who handle the records would have a duty to avoid disclosing their contents to anyone except the affected patients.

The statutory protections must be drafted broadly enough to include the non-medical as well as the medical information which is contained in these records. So often various categories of social data are collected because of their assistance in diagnosis and treatment. If such matters were not accorded the recommended protections, there might be a concomitant and harmful temptation for patients to withhold the data from their doctors.

The principles upon which this position is based can be summarized as follows. First, as an incident of human dignity, a patient ought to have the right of access to the most personal information about himself or herself. No person, even though he or she may be a professional with much knowledge and experience, should be entitled to withhold that information. Second, the patient in his or her own interest, should be able to correct any misinformation which may appear on his record. Third, the patient will have a better understanding of his or her treatment and be in a better position to assist in future care. Fourth, access to the file will allow a patient to make an informed consent to the release of information from the file to a third party when necessary. Fifth, access creates a feeling of trust and openness between patient and health-care providers, and the quality of health care will thereby be enhanced.

One of the most frequent arguments advanced by those who opposed direct access by patients to their own health records is that it is not in the best interests of the individual to have access to his or her record. It was suggested that some of the information in the record could be misleading to the patient or could bring about harm to the patient, the provider of the information, or to a third party. Examples given in support of this argument purported to show that harmful consequences would result from patient access. Few cases of actual harm, however, were given. In its written brief, The College of Physicians and Surgeons of Ontario gave this example:

It is common in Ontario for the physician to enter in his medical records the service for which he has billed the Health Insurance Plan with respect to the patient's visit.

There has been a case in which a physician noted the service of psychotherapy, only to have the patient subsequently lodge a complaint that the use of that term was defamatory to him, since he had never suffered any mental illness. The patient simply did not know that psychotherapy as a procedure does not carry any connotation of mental illness and was not so intended by the physician. Nevertheless, the physician was required to defend himself against such a complaint, and the relationship of confidence which had existed between the patient and that physician was utterly destroyed.

Another illustration used by the College was that, "the term 'S.O.B.' when used by a physician to record shortness of breath may be misinterpreted by the patient as a derogatory reference to him." In these examples, the misinterpretations are the results of the terminology used. Habitual use of jargon or technical terminology is not, in my view, a sufficiently sound reason for failing to establish a salutary practice. A re-evaluation of the methods used in record keeping, may, however, be necessary.

A compromise solution proposed by several individuals and organizations opposing direct access would grant a right of access through an intermediary or interpreter. The Ontario Medical Association suggested that access "be only through his attending physician or another physician with responsibility for the patient's care." The Canadian Health Record Association qualified its position on patient access similarly, as follows:

We feel it is appropriate that the provider of the health care be advised in advance, and that there be a person available to interpret the contents of the record to the patient who wishes to see his record.

An interpreter, whether it be the attending physician or other health-care provider, can serve a very useful purpose if the patient desires his or her service. However, as I indicated above in my discussion of the proposed U.S. legislation, I do not support the requirement as a condition of the general rule of access.

The College of Physicians and Surgeons of Ontario presented this position with respect to patient access:

It would seem reasonable and desirable to afford the patient access to information contained in the medical record to ensure completeness, subject to controls designed to prevent such a disclosure from being more harmful than beneficial. There are very serious concerns within the profession of medicine that direct patient access to medical records would be detrimental to the very quality of these records, and thus to the quality of health care.

While society's attitude toward access to information generally has changed in recent years, professional attitudes have changed much more slowly. Patients are much more knowledgeable about their health care than they were 50 years ago. Many physicians who appeared at the hearings stressed that good patient care depended upon complete frankness on the part of the patient. While I believe that statement to be incontrovertible, it is my opinion that good medical care requires a reciprocity in which the physician, if asked so to be, is completely frank with the patient. If the patient asks to see his or her record, is informed by the physician of any risks and harmful consequences of doing so, and is nevertheless willing to run the risk, no amount of paternalism should stand in the way of the right of access. The following discussion, which occurred at one of our hearings, with Dr. Douglas Y. Caldwell, then president of the Ontario Medical Association, is instructive:

MR. COMMISSIONER: For example, it is conceded, I think, throughout by everybody who has appeared here who is a member of the medical profession that if in fact a patient is advised by his physician and surgeon, or by a surgeon, that the patient needs surgery, if the patient is in fact under no legal disability, and refuses surgery, everybody concedes--as I recall the evidence, I don't think there was any exception to this--everybody concedes the patient is entitled to refuse to do something which in the opinion of his medical advisor he would be very silly to refuse.

DR. CALDWELL: It is his right to refuse.

MR. COMMISSIONER: It is his right to refuse, yes. If it is his right to refuse,

then why shouldn't he have a right, even if it would harm him, to see what you have in your file about him?

DR. CALDWELL: I suppose one could say that....

A persuasive case using this analogy is made by Professor Terence G. Ison, in his paper, Information Access and the Workmen's Compensation Board, prepared for the Commission on Freedom of Information and Individual Privacy, January, 1979. At page 84, he states:

One would think, for example, that an unfortunate choice by a patient with regard to treatment could be more disastrous than an unfortunate choice regarding access to records. Yet the profession makes no similar claim to a right of ultimate decision.

When the question is, for example, whether a patient should have an operation, the patient seeks advice from the doctor, but both recognize the ultimate right of the patient to decide for himself. Why should the same principle not apply to medical records? A possible answer is that the doctor, having seen the file, is in a better position to assess its likely impact on the patient. But the same is true with operations. Yet the superior knowledge and superior ability of the doctor to predict the likely consequences are not used as arguments to deny a patient's right to decide for himself.

Health records that contain information about more than one person present a special problem. For example, access to the record by a member of a family may reveal information which another family member may have compelling reasons to keep confidential. This was stressed in our discussions of genetic counselling and patients' sexual problems. I was informed by a physician of a case in which, after discovering a genetically transmitted disease in a child, he examined all members of the family. The child's mother later returned to inform him that the affected child was not in fact her husband's child. To record this information on a record to which the mother's husband might have access would create an obvious potential problem. A similar problem would arise if the information were to be recorded in a family record. In some situations, it seems



clear, there may be a justification for refusing complete access.

Section 11 of The Public Hospitals Act, provides that:

The medical record compiled in a hospital for a patient or an outpatient is the property of the hospital and shall be kept in the custody of the administrator.

Some hospital administrators rely on this provision to deny access. Although the physical record may belong to a hospital, it is the information in the record that is in question. That the hospital owns the record is not an answer to the patient's claim of entitlement to inspect the record or obtain a copy of it. As The College of Physicians and Surgeons stated in its submission,

It seems clear that the physician owns the office records which he prepares, but it is equally clear that the patient has an interest in the information contained in those records.

I have already referred to the view expressed by Mr. Justice Maloney in Re Mitchell and St. Michael's Hospital, to the same effect.

From our examination of the by-laws of public hospitals in Ontario, and from the testimony given by hospital administrators, the conclusion may be drawn that patient inquiries about their own records are discouraged. In most hospitals, the attending physician determines whether the hospital record may be released to the patient. Under The Public Hospitals Act, "the board" is given a discretion with respect to the disclosure of medical information to "a person" with the patient's consent. I repeat again that I am of the view that the words "a person" include the patient. However, hospitals prefer the individual to channel his or her request through a third party, usually a lawyer. The following discussion took place at our hearings with the administrator of a large community hospital in Metropolitan Toronto:

MR. STROSBURG: You have already said that if it is a standard motor vehicle case and the solicitor writes in saying I am acting for Joe Smith, might I have copies of the medical records. As a routine, they are

generally forwarded. You have already said that?

A. To his solicitor.

Q. To a solicitor.

A. Yes.

Q. But if Joe Smith writes in himself and says he wants copies of the records he is generally told, why don't you go talk to your doctor?

A. Yes. And we will contact the doctor too, because we don't feel it proper that patients are in limbo as far as what their condition is. We feel it very important that the patient know and have knowledge clearly and authentically as to what happened to him and what treatment they had. We feel the person best able to give that is the physician who gave the treatment or the physician who knows the patient best.

Q. Or the lawyer?

A. Well the lawyer, I feel the lawyer, we give the lawyers credit for perhaps things that we may not, maybe we shouldn't credit them with. But let me say this, we assume that the lawyer will use good judgment in regard to his client as to the effect of any knowledge or the bad effect that such knowledge might have on him. Now we are crediting the lawyer, we treat the lawyer a little differently in that case because he is certainly not a medical practitioner but we usually conclude that he is probably a wise person and if he was in doubt about the patient's reaction to information he would handle it in the proper way for the benefit of his patient.

Q. All right. Now, is not the lawyer's right to have access to the records no higher than his client's?

A. The record, the lawyer wouldn't get the record if the client didn't authorize it.

Q. Yes, so that his right to have the records depends upon the authority of the patient?

A. Yes, yes.

Q. So why would you put the lawyer in a higher position than you put the patient himself?

A. Well I guess I am not explaining this very well.

MR. COMMISSIONER: Yes you are. But the problem is--I don't think there is any doubt about what you are saying--but the problem is...you say maybe we are attributing to the lawyer better judgment than we ought to. You are according him a status which he doesn't have. The fact that a man or a woman is a lawyer does not give that person any greater rights than anybody else in society, and in the sense that he or she is simply the alter ego of the client, and what you're saying is we will tell the lawyer because the lawyer may withhold information from the patient which he thinks the patient ought not to have. What we are finding is that that's a fairly common view....Lawyers seem to be accorded a status by virtue of their entitlement to practise law which causes hospitals to give them information which they will not give their clients. I am frankly puzzled by it because I understand that the lawyer's obligation to the client is to be fully frank with the client, and I don't know what right a lawyer has to say, "I've got all this information about you on your authority from the hospital, but I'm not going to let you know about it."

. . . . .

A. I don't know if I can convince you. I would expect that you are going to see many witnesses who would be better able to speak

to this than I am. Maybe more convincing. I think it is not the intention to accord the lawyer with any status that is higher or more elevated than the patient. It is simply that we do feel that there is some probability that the lawyer is pretty wise in his judgments as respects that patient. If he would not, that the information in that case is for the benefit of the patient and not to harm the patient. I think that the feeling is, and again you will be speaking to physicians who will be better to speak to this, that they are not anxious to give the lawyer, information to the lawyer and a feeling that the lawyer is more entitled than the patient. It is simply that if he judges that there could be something in the information that would be worrisome for the patient, not just a legal matter but that the lawyer would then perhaps consult with the physician and try to clarify this issue before he upsets the patient.

Now maybe this is, as I say, I think that's the theory and whether it is a highly inflated theory or not, I don't know.

MR. COMMISSIONER: Doesn't the theory reflect a very paternalistic view with relation to the patient? In your own interest we are not going to give you this information, but we'll give it to your lawyer. Maybe some patients say I don't want my lawyer to know. I want to know this information. Why, for example, if I were a patient in your hospital and I wanted to know precisely what the records said about me, why should you deem it imprudent on my part to have that information unless there is the intervention of a third party such as a lawyer? Why should I have to go to Mister Strosberg and say, "Here, I am going to give you authority. Would you on my behalf write a letter to Mister McCarthy and get my hospital records, because they will give it to you automatically."

A. Okay. Sir, could I just tell you that first of all we feel, or I feel, I guess I better just speak for myself, that the best person to explain the situation is the physician who knows the terminology, who knows what the drugs mean, he knows the consequences of these things and who would explain it. We, I would think that in many, many cases the record would be meaningless directly to the patient without some kind of interpretation of what does this obscure number on this lab form mean. I think I wouldn't pretend to know what it means either. So, although I am associated with the hospital I would be among the many people who don't understand the consequences of the many sophisticated tests and things that are done. So the final note, of course, usually summarizes all of this and we would hope that the physician would convey to the patient the information that is in his final note which summarizes what the patient's diagnosis was and what treatment was done and what his direction is for the future.

MR. COMMISSIONER: Yes, but do you give it to Mister Strosberg? He doesn't know what an elevated BUN means, any more than I do.

A. Sir, I thought I explained that before. We don't deny the patient. We would simply say to the patient, "Look, have you talked to Doctor Jones"--who was the physician attending them in the hospital--and if he says no or if he says, "I talked to him and I wasn't satisfied," we will get in touch with the physician, as I explained in that particular case, and try to convey to the patient--in this case it was the son of the patient--an explanation of what happened.

If it goes beyond this, you're saying, well, the patient now is still not satisfied. We have done all we can to facilitate the flow of information. We simply say if you are, we say to the patient, I think it's safe to say, "If you are not, we have done our very best to inform you. We are not prepared to



give you your medical record, our medical record on you, and if you want it you may, we would release it to your lawyer on your authorizing him," and that's the way we leave it. Now whether we are right or not in that...

MR. COMMISSIONER: When the lawyer writes you don't call in a physician to try to persuade the lawyer that he should only have certain information. You give the lawyer the information.

A. Yes. Yes.

MR. COMMISSIONER: What I am saying is, why can't you accord the patient the same respect that you accord his lawyer who may be more ignorant than the patient in medical matters?

A. Sir, I wouldn't. I don't, I respectfully take issue with the word lack of respect, because in my opinion we do not view it as respect or non-respect.

MR. COMMISSIONER: No, I didn't mean to imply that. What I am saying is you have a paternalistic concern for the welfare of the patient, which you don't exhibit when the patient has a lawyer.

A. I guess I said that before. We feel that the lawyer is first of all a little removed from the case. He has an interest in the patient, and I'm sorry, he is interested in his client, an obligation to his client, he will do whatever, in consultation with his client he will make the best judgment he can. If he is not satisfied that he understands what is in the record, he can speak to the physician. He can call a medical, consult with some other physician. He has many avenues that sort of assure him, I suppose these would be open to a patient as well, to speak to another physician.

MR. COMMISSIONER: Certainly. I could ask Mister Strosberg to write a letter to you to

get a medical record. Then when he got it, I could say, "Give it to me. I instruct you, you are my solicitor, you have to do what I say, give me my record." He can't say, "No, I am making a judgment that you ought not to have that which you instructed me to get for you."

In the same discussion, when asked if the hospital would forward a copy of the record to the patient's lawyer, if the patient so directed, in a case in which it was suspected that the patient contemplated suing the hospital, the administrator said that the information would probably not be provided. When asked why, he said that to do so would not be in the patient's best interests because it would facilitate frivolous lawsuits. He saw no conflict of interest in the hospital's determination that, in those circumstances, it was not in the patient's best interests to be provided with a copy of the record as requested.

In the arguments made in favour of access, it is pointed out that if the record is misleading to the patient, it may be even more misleading to third parties who may be given access. It is further argued that along with a right of access must come the opportunity to correct any misinformation in the record, without which incorrect information may be passed on to other parties with unfortunate results. One case brought to our attention was that of an employer who had received medical information that a prospective employee had suffered from alcoholism. Although it was later discovered that the information received by the employer was incorrect, the employee had been refused the job because of the information. If the individual had had an opportunity to see and correct the misinformation, given the qualifications of the applicant, there would have been a different result. Professor Cyril Greenland of the School of Social Work and the Department of Psychiatry of McMaster University gave this evidence:

Yes. Perhaps I could just add to that by saying that the, that it does happen sometimes, and it is regrettable, that inaccurate information is contained in files, and if you ask me how do you know that, I would answer that in 1967 I had an opportunity in Britain to sit in on a hundred or so review tribunal hearings when this issue was often a matter of conflict. Where the chairman of the tribunal allowed access to clinical records, the patient and/or his

relative would often be able to pinpoint information that simply was not true, or at least if it wasn't true it was not...for example, the record would say that this particular patient was in a fight, indicating his propensity to violence, and that statement simply stood alone. When the patient was given an opportunity to say what exactly happened, then sure enough there was a fight, but someone else may have instigated the fight and yet the way the document is presented he had to take all the blame for this. And in many of these cases the nurses who were witnesses, who were called, and their account of what actually happened coincided with the view the patient presented and not with the view that was in the psychiatric record. So in terms of the accuracy of the record it seems to me absolutely vital that the patient, his relatives or whoever represents the patient or his relatives must have access to that if justice is going to be done.

I would say that before doing that study, and I spent over a year at this, I would have as a therapist, because that is my background, I would have had some qualms about making these records available. But now that I know something about the lack of accuracy of the material contained in the records, my view has changed entirely.

The question of access to psychiatric records sparked the most vigorous debate on this issue, and has given me considerable concern. Although, as a society, we have done much to remove the stigma that was once associated with mental illness, it would be unrealistic to say that the enlightened view of mental illness is now universal. It is inconsistent with the view that illness is illness, whether it be mental or physical, to make a distinction between records which are kept with respect to physical health and records which relate to mental health. (I consider the special position of a patient under a Lieutenant Governor's warrant in my discussion of the Advisory Review Board.)

One position taken by representatives of the field of psychiatry was that seeing a record containing psychiatric information could cause a patient more harm than seeing information

dealing with a purely physical illness. The ad hoc committee of the Department of Psychiatry, University of Toronto, made this argument in its brief:

A special circumstance occurs when the patient himself desires to view his own records. It is the opinion of this committee that such access is not always desirable and could be damaging to the patient. If such free access were permissible, the material of the records may become highly censored so as to include only those items which the patient may view. Hence, the records would cease to be meaningful accounts of the patient's true state. The records include objective and subjective material essential to make a diagnostic formulation and equally essential to the nature of psychotherapeutic work. Also, they may contain statements by relatives about the patient which were given in confidence by a relative.

Therefore, these records comprise not only data emanating from the patient but also include formulations by the therapist as he interprets the data he receives. The therapist himself has rights of privacy relevant to this latter material. The records also contain reports by psychologists, social workers and nurses which were made in the belief that they would not be directly released to the patient.

There may be some exceptional circumstances where it is helpful for the patient to see his own records together with the therapist who will interpret the material for him. However, it is a fact that the records are the property of the therapist (or his hospital) and cannot be viewed without the consent of the property-owner, i.e., the therapist in a private practice or the hospital authority, except by means of subpoena.

In its helpful brief, the Clarke Institute of Psychiatry provided examples of types of situations in which it would be opposed to an unqualified right of access:

### 3.1 Third Party Information

(a) The mother of a very depressed adolescent confides in the social worker about an affair she has been having for several years. She is sure her husband does not know about this. We are reasonably sure that the son does not know about it. There is some thought that the patient's illness is related to the tension and the distance between his parents. Revelation of the above information to either patient or husband would constitute a serious breach of trust.

. . . . .

(c) A 16-year-old boy lives with his grandparents whom he believes to be his parents. Actually, his birth was the result of an incestuous relationship between a brother and sister. The treating doctor sees no benefit in revealing these historical details to the patient.

. . . . .

(f) This patient is a 34-year-old woman with a long history of multiple drug abuse, paranoid delusions and menacing behaviour.

She was treated for two years in the Ambulatory Service of the Clarke Institute. During this time the police circulated the photograph of a suspected criminal and the outpatient staff thought the photograph bore a strong resemblance to the patient. This possibility is outlined in the progress notes, as is the advisability of contacting the police. As it happened, the patient was arrested on another charge, was cleared of the suspicion of murder, and subsequently terminated her involvement with the Institute. Because of her paranoid personality and recurrent suspicions, she periodically returns and asks to see her clinical record because, she feels, Clarke staff "have done her in".



It continues to be the conviction of all concerned that it would be in neither the patient's nor the staff's best interests to allow her to read about ther staff's one-time suspicion that she might have been the criminal the police were seeking.

. . . . .

(i) A married couple were seen together for the most part, and occasionally separately. An extremely destructive and vindictive separation was followed by threatened legal action over custody and alimony. The husband wanted his clinical record to prove his wife's instability and incompetence. The joint sessions had been recorded in his clinical record. It would have been both unethical and destructive to allow him access to his clinical record.

### 3.2 Technical Language

A patient with recurring psychotic episodes "stole" his clinical record. He took it from his doctor's desk, read it thoroughly, and returned it. It has seemed as if, since that day, the patient has been unable to trust psychiatric staff. He refers to the medical terms he read in his record, i.e. "paranoid", "manic", "schizophrenic" and interprets them as pejorative labels that have been affixed onto him by "arrogant, uncomprehending" staff. It has not been in this patient's best interest to have gained access to his chart.

### 3.3 Inferred (Unconscious) Motivation

(a) a young female inpatient was given a sodium amytal interview by her doctor. The interview did not reveal any new facts. However, a lot of material in relationship to her mother was of so depressing a nature that it seemed to be impossible for the girl to absorb it. For example, when she was pregnant her mother was hoping that she would not indeed be pregnant, but that the swelling in her abdomen would be a tumour.

She told this sad story with a laugh and it seems that she is strongly defended against looking at any of this material. We do not intend, at this point in time at least, to probe it because we feel sure she will not be able to deal with the degree of depression the probing would elicit. Currently she is weakened by chronic nephritis and other physical illness.

### 3.4 Preliminary Conclusions

(a) a university student with very poor self-esteem was being seen as an outpatient. Therapy was designed to be reassuring and ego-building. Not expressed to the patient, but confided in the chart, were the therapist's opinions about this patient's intellectual capabilities and his abilities to complete successfully his university course. The patient also had sexual orientation problems which he had asked the therapist not to note in the record "in case it fell into the wrong hands". In deference to the patient's wishes, this area of difficulty was therefore not entered into the clinical record but the patient, wanting to check this point, asked to see his clinical record. Because of the references to the patient's intellectual ability which, it was felt, would not be in the patient's best interest to read, the patient was not given access to his record.

. . . . .

(c) There are examples of cases in which parents accuse each other "on behalf" of the child. A specific case in point is a recent custody access case in which we have assessed a 6-year-old boy whose mother is denying access to father. Presently, you will find on the record of this boy that his father accuses his mother of being a lesbian while the mother accuses the father of being pedophilic. As yet, we are uncertain whether these accusations are grounded in reality and we ask about the relevance of this information in the child's clinical

record and furthermore whether such information should be conveyed to the children at any point in the future.

The position of the Clarke Institute of Psychiatry was put this way:

Clarke Institute of Psychiatry favours the principle of open, frank and honest communication between providers and consumers of health services. In the doctor-patient relationship, especially in psychotherapy, high value is attached to open self-disclosure by the patient and to disclosure to the patient by the doctor of information that emerges about the patient in the course of treatment.

Nevertheless there are situations involving both outpatients, and most especially inpatients, where patients' clinical records contain preliminary and interim professional opinions, reports from third parties, results of laboratory investigations, and so on, which should not be made available to the patients. The hospital clinical records are working documents that contain material of potential value to members of the treating team, and they are collected with this aim in mind. If patient access to these records were likely, the files would have to be assembled in quite a different way. Both the quality and content of record keeping would change drastically and material of potential value would have to be excluded. This could in some cases adversely affect patient care.

The fear has been expressed that record keeping practices, and therefore records, would change if access were allowed. Professor Greenland addressed this question in this fashion:

As a general principle, I would say in response to your honest question that there should be open access as far as is humanly possible, and there must be some very, very exceptional reasons where access to this information would be denied. Now I think that there might be exceptional reasons

existing, but this would be a rare event rather than a usual event, and my general feeling would be that access to information should be available to patients and their relatives or people representing them.

There is now in the psychiatric literature several articles on this topic where patients have had access to their clinical records as patients, and all the kinds of concerns that clinicians and others have had about the harm that this might do is found in fact to be fantasy. In fact, it improves the situation rather than hurts the relationship. What happens in fact is that the notes of clinicians and others become much more objective in this situation when the record is available, and I think this is all to the good.

Dr. Nahum Spinner, Professor of Psychiatry at McMaster University, at our hearings at that university, spoke of the benefits that a policy of access to their records by psychiatric patients would bring:

But I would argue that this difference perhaps might lead one to think that in psychiatry, more than anywhere else, the patient ought to have access to records. Because a great deal of psychiatric treatment, especially psychotherapy, consists of helping the patient to correct distortions in perceptions of himself and his place in the world. A great deal of that psychotherapeutic work really consists of helping the patient see how others see him. The others may be wrong, but how they see him is nevertheless a piece of reality which affects his life and his reactions, and very gravely.

So that in fact, the process of psychotherapy consists in an ongoing communication to the patient by verbal means, of his medical record. It's extremely difficult for me to imagine a situation in which information which is professionally sound and ought to be in the record ought not to be accessible to the patient. There is

disagreement about a paranoid patient. I myself, share the view that you have suggested, that paranoid people in general are made more paranoid if they do not have access to everything we know and are into the field of totally open communication.

But I would argue that...and that, incidentally has been proven. For over two decades now there have been teaching hospitals in the United States in which the patient participates in clinical rounds and absolutely nothing, nothing at all that any professional says about a patient is not said in the presence of the patient. If, for example, one has information that this patient is epidemiologically speaking a high risk of suicide, a male over fifty, living alone, is apparently a suicide risk all the statistics say. There is a good deal to be said in favour of thinking that sharing that risk with the patient may prevent rather than precipitate the feared consequence.

So in psychiatry I think that, despite the great resistance which the profession would put up, that making the records accessible to the patients would have two consequences. One is it would reputedly greatly improve the quality of the records. Secondly, it would in itself be therapeutic.

Reference has already been made to the development of policies in other jurisdictions allowing patients access to their own records. In this connection, the experience of Saint Elizabeths Hospital in Washington, D.C. is interesting. That institution is a federal psychiatric hospital with approximately 2,000 in-patients and 3,500 out-patients in 1978. Approximately 10 per cent of the patients are in the Division of Forensic Psychiatry. Approximately four years ago, the hospital, governing itself by the provisions of the U.S. Privacy Act, adopted a procedure by which patients are shown their records upon request, without exceptions, despite the fact that the legislation allowed for exemption if a physician deemed access not to be in the best interests of the patient. Before this procedure was implemented, there had been many expressions of concern on the part of the staff of Saint Elizabeths that harm would come to patients as well as staff members. The number of requests for access to their files by patients was not as large as expected.



At the time of our enquiries, there had been 200 requests for access by patients throughout the three years the policy had been in effect. The total number of patients during the period was between 10,000 and 12,000. Members of the hospital staff did find that their attitude toward record keeping had changed to a certain extent and that they had to set up regularized procedures for an individual to apply for access to his or her file. The patient's right to access is included in the patients' rights statement distributed when a person becomes a patient. Some of the hospital staff were enthusiastic about the access policy, while others found the additional clerical workload onerous. However, the prevailing response, even for those who had been concerned about its consequences, was one of acceptance of the policy.

As an appendix to its written submission, the Ontario Hospital Association submitted a document which was a joint working project with the Ontario Medical Association and in which the following statement is made reflecting another concern which I share:

It is essential that undue access to such information does not inhibit the complete recording of adequate and valuable data necessary for the continuing care of the patient.

I say, at once, that I do not believe that any responsible and ethical physician would omit from a medical record any information that, in the interests of proper medical care, belongs in it because of the possibility that the patient may ask to inspect it. Some physicians have expressed the view that patient access may cause the creation of two sets of records, one for the patient's eyes in the event he or she asks for it, and the other for the physician's own use. Others, on the other hand, have said that the quality of record keeping will be improved. A representative of the Patients' Rights Association probably accurately reflected patients' expectations on this issue:

MR. COMMISSIONER: ...What I am asking you to do is relieve me of the worry that the quality of care will in some way be impaired because the record will not be what it should be.

MRS. COY: Mister Commissioner, don't you think the key word here on page seven is 'accurate'? "Health professionals and institutions are under statutory duty to

keep accurate records". And I don't think it matters whether there is superfluous information in there. If the information is accurate, and I think that that is all that a patient would ask about his own record, that the information in it be accurate, and I would feel that a conscientious physician will keep an accurate record.

The Canadian Civil Liberties Association made this suggestion:

The law should specify what categories of information must be recorded for patient access and such items should be subject to expansion, but not reduction, by regulation.

Whatever merit this proposal may have, the content and form of medical records lies outside the scope of my terms of reference.

To conclude by referring again to the legislation in other provinces, with respect to the principle involved, the example set by Alberta, Quebec and Nova Scotia is one well worth following. Especially commendable is the provision in The Alberta Hospitals Act, which places on the respondent the onus of showing why disclosure ought not to be made to the patient, when the patient applies to the court for an order directing the release of the information. The Ontario Medical Association's support for a mechanism similar to that in Alberta, if there is to be patient access to medical records, is, in my view, an enlightened position. It is, moreover, a position for which I have considerable sympathy. However, it has a serious shortcoming. An application to a court, even by way of originating motion, is expensive and might well be beyond the ability of an interested patient to afford. Even if one takes the more desirable course, that of placing the burden on the institution or the physician to apply to the court for an order permitting it, him, or her to refuse production of the patient's health information, a significant expense is still involved. It is difficult to justify a procedure that puts, say a physician, to an expense which he or she must bear personally when that physician is resisting production out of a concern for the best interest of the patient, or, in certain cases, of a third party. On the other hand, to refuse the courts any role is to overlook an institution that is justifiably regarded by most members of society as an objective and impartial decision maker. Certainly a health professional or institution would not be considered to be entirely free of bias. Because of the desirability of avoiding the incurring of legal costs by the parties, the courts

should be a last resort. An intermediate mechanism should be brought into existence. The creation of an office of Health Commissioner, who might, in the course of time, be given other responsibilities in our health-care system, is a convenient solution to the problem I have described. This person, a respected man or woman, who should not be a member of a health profession or occupation, can, informally, expeditiously and inexpensively, without any necessary involvement of lawyers, be given the responsibility of entertaining applications by physicians or health-care institutions for exemptions from the general duty to allow patients access to their health information. An appeal from the decision of the Health Commissioner should lie to the County or Supreme Court.

*Recommendations:*

82. That legislation be enacted to express the general rule that an individual has a right to inspect and receive copies of any health information, of which he or she is the subject, kept by a health-care provider.
83. That a Health Commissioner, a well-respected, non-member of the health professions, be appointed, whose responsibilities would include receiving applications by health-care providers for an exemption from the obligation to disclose information to a requesting subject, receiving applications by an individual for corrections to his or her health information, making a decision on the applications, and informing the health-care providers and the subjects of the decision.
84. That when, in the opinion of the health-care provider, disclosure of the information is likely to have a detrimental effect on the physical or mental health of the requesting individual or other person, an application may be made by the health-care provider to the Health Commissioner for an exemption from the obligation to disclose that information. The decision of the Health Commissioner should be subject to an appeal to the County or Supreme Court.

85. That, after inspecting or receiving the health information, an individual have a right to request that the information be corrected. The health-care provider shall make the correction as requested or inform the individual of the reasons for the refusal. In the event of a refusal, the individual may apply to the Health Commissioner for review of the refusal. The decision of the Health Commissioner should be subject to an appeal to the County or Supreme Court.

## Psychiatric Records and the Advisory Review Board

In recent years the conflict in the competing interests inherent in the very concept of involuntarily hospitalization of some mentally ill patients has drawn the attention of an increasing number of members of our society who have had reason to question the need for the deprivation of liberty of some mental patients. Although far from local, this concern has resulted in the amendment of The Mental Health Act, R.S.O. 1970, chapter 269, and the creation and report of the Committee on Mental Health Services in Ontario. Indeed, these concerns arose first in the U.S.A., and their appearance in Ontario may well be part of a North American phenomenon. They are, in fact, directly related to the due process movement as it relates to the mentally ill who have been committed to psychiatric institutions, in most instances, under statutory provisions dealing with involuntary civil committal.

There is probably a relationship between the emergence of some of the problems to be discussed and the development in Ontario of a small Advisory Board of Review Bar, a group of lawyers dedicated to ensuring that the principles of due process are observed when the cases of the involuntarily committed patients are being considered. These lawyers are clearly familiar with developments in the field in the U.S.A. and reflect a valid point of view. To illustrate the nature of the problem I am addressing, I quote from a recent letter to the Advisory Review Board from a lawyer representing a patient whose case was recently the subject of consideration by the Board:

...Without an opportunity to examine the Clinical Record and determine what if any allegations contrary to his interests are contained therein, I am unable to properly represent Mr.                    during the course of his hearing before the Advisory Review Board. Accordingly, as I have done in the past, I would respectfully request that the Board provide me with disclosure of all written or oral information made available to any or all members of the Board prior to or during Mr.                    's hearing this year and that such



disclosure be made well in advance of the scheduled hearing date so that I might have an opportunity to adequately prepare to respond to such material by cross-examining the persons involved, calling witnesses or such other means as may seem appropriate.

The request contained in the letter from which I have just quoted raises two questions. The first has to do with the right of the Advisory Review Board itself to see the patient's clinical record, and the second with the right of the patient or his or her counsel to see it. The answers to both questions are, at the moment, anything but clear. The practice has been, and continues to be, that the Board does have before it the hospital's file or the clinical record at the time of the hearing and during its deliberations. The way in which the problem arises will be better understood after a brief discussion of the constitutional basis of the Board in Ontario and it is to that troublesome question that I now turn. Before doing so, I pause to point out that the words "clinical record" were introduced into The Mental Health Act by The Mental Health Amendment Act, 1978, S.O. 1978, chapter 50. Section 10 of that Act, now section 26a of The Mental Health Act, defines "clinical record" as meaning "the clinical record compiled in a psychiatric facility in respect of a patient, and includes part of a clinical record."

Most of the Boards of Review in Canada were created under the authority of section 547 of the Criminal Code, R.S.C. 1970, chapter C-34, as amended by S.C. 1974-75-76, chapter 93, section 71. Section 547 reads as follows:

547.(1) The lieutenant governor of a province may appoint a board to review the case of every person in custody in a place in that province by virtue of an order made pursuant to section 545 or subsection 546(1) or (2).

(2) The board referred to in subsection (1) shall consist of not less than three and not more than five members of whom one member shall be designated chairman by the members of the board, if no chairman has been designated by the lieutenant governor.

(3) At least two members of the board shall be duly qualified psychiatrists entitled to engage in the practice of medicine

under the laws of the province for which the board is appointed, and at least one member of the board shall be a member of the bar of the province.

(4) Three members of the board of review, at least one of whom is a psychiatrist described in subsection (3) and one of whom is a member of the bar of the province, constitute a quorum of the board.

(5) The board shall review the case of every person referred to in subsection (1)

- (a) not later than six months after the making of the order referred to in that subsection relating to that person, and
- (b) at least once in every twelve month period following the review required pursuant to paragraph (a) so long as the person remains in custody under the order,

and forthwith after each review the board shall report to the lieutenant governor setting out fully the results of such review and stating

- (c) where the person in custody was found unfit on account of insanity to stand his trial, whether, in the opinion of the board, that person has recovered sufficiently to stand his trial,
- (d) where the person in custody was found not guilty on account of insanity, whether, in the opinion of the board, that person has recovered and, if so, whether in its opinion it is in the interest of the public and of that person for the lieutenant governor to order that he be discharged absolutely or subject to such conditions as the lieutenant governor may prescribe,

(e) where the person in custody was removed from a prison pursuant to subsection 546(1), whether, in the opinion of the board, that person has recovered or partially recovered or,

(f) any recommendations that it considers desirable in the interests of recovery of the person to whom such review relates and that are not contrary to the public interest.

(6) In addition to any review required to be made under subsection (5), the board shall review any case referred to in subsection (1) when requested to do so by the lieutenant governor and shall forthwith after such review report to the lieutenant governor in accordance with subsection (5).

(7) For the purposes of a review under this section, the chairman of a board has all the powers that are conferred by sections 4 and 5 of the Inquiries Act on commissioners appointed under Part I of that Act.

Of the 10 provinces, only Newfoundland and Prince Edward Island, do not have Review Boards. Of the remaining eight provinces, the Review Boards of five are constituted under section 547 of the Criminal Code. British Columbia's Board owes its existence to an order-in-council that does not relate to any statute and those of Saskatchewan and Ontario were created by orders-in-council made under the authority, not of the Criminal Code of Canada, but of provincial mental health legislation. In at least two of the provinces, Quebec and Alberta, the Boards are not "advisory" in the sense that they report to Cabinet which advises the Lieutenant Governor, but report directly to the Lieutenant Governor. Political involvement is thus absent. For Boards created under the Criminal Code, the right to inspect the hospital's file or the clinical record may not be difficult to determine. Although it appears that those Boards that do have access to these records have it voluntarily, subsection 7 of section 547 gives them the power to compel production, for it incorporates by reference sections 4 and 5 of the Inquiries Act, R.S.C. 1970, chapter I-13. These sections are in the following language:

4. The Commissioners have the power of summoning before them any witnesses, and of requiring them to give evidence on oath, or on solemn affirmation if they are persons entitled to affirm in civil matters, and orally or in writing, and to produce such documents and things as the commissioners deem requisite to the full investigation of the matters into which they are appointed to examine.

5. The Commissioners have the same power to enforce the attendance of witnesses and to compel them to give evidence as is vested in any court of record in civil cases.

Ontario's Board was created by provincial legislation before the enactment federally of the power of the Lieutenant Governor to appoint a board of review. The provincial legislation, in its present form, is found in section 31 of The Mental Health Act. That section provides as follows:

31. (1) The Lieutenant Governor in Council may appoint an advisory review board for any one or more psychiatric facilities that has a review board.

(2) An advisory review board shall be composed of a judge or a retired judge of the Supreme Court who shall serve as chairman, a psychiatrist and any three members who constitute a quorum of the review board.

(3) Subsections 4, 5 and 6 of section 27 apply mutatis mutandis to the members of an advisory review board.

(4) The five members of an advisory review board constitute a quorum and the recommendation of a four-fifths majority is the recommendation of the advisory review board.

(5) The case of every patient in a psychiatric facility who is detained under the authority of a warrant of the Lieutenant Governor under the Criminal Code (Canada) shall be considered by the advisory review board having jurisdiction once in every

year, commencing with the year next after the year in which the warrant was issued.

(6) Notwithstanding subsection 5, the advisory review board shall consider the case of any patient to which that subsection applies at any time upon the written request of the Minister.

(7) Section 29 applies mutatis mutandis to cases under this section.

(8) Upon the conclusion of an inquiry, the chairman shall prepare a written report of the recommendations of the advisory review board and, within the time prescribed by the regulations, shall transmit a copy thereof to the Lieutenant Governor in Council, and may in his discretion transmit a copy thereof to any other person.

Section 29, incorporated by reference, by subsection 7 of section 31, appears to be the basis of the Board's power to examine the hospital or clinical record--see subsection 4 set out below--but, and this is curious indeed, it was repealed by S.O. 1978, chapter 50, section 11, and replaced by a provision that deals with an entirely different subject. The repealing enactment, however, has not yet been proclaimed and for the time being the Board enjoys the power to require the officer in charge of the institution to furnish such information as the chairman requests. Whether that power entitles the Board to the clinical record, is, however, very much in doubt. I shall return to this point later in the discussion. In the meantime, I set out the language of section 29 and direct special attention to subsection 4.

29. (1) Upon receipt of an application by the chairman, the review board shall conduct such inquiry as it considers necessary to reach a decision and may hold a hearing, which in the discretion of the review board may be in camera, for the purpose of receiving oral testimony.

(2) Where a hearing is held, the patient may attend the hearing unless otherwise directed by the chairman and, where he does not attend, he may have a person appear as his representative.



(3) Where a hearing is held, the patient or his representative may call witnesses and make submissions and, with the permission of the chairman, may cross-examine witnesses.

(4) The officer in charge shall, for the purpose of an inquiry, furnish the chairman with such information and reports as the chairman requests.

(5) The review board or any member thereof may interview a patient or other person in private.

My immediate concern is to refer to the current uncertainty about the constitutional basis of a Board appointed under provincial legislation, now that power to create a Board is contained in the Criminal Code. The cause of the uncertainty is a recent decision of the Divisional Court in Re Abel et al. and The Director of Penetanguishene Mental Health Centre; Re Abel et al. and The Advisory Review Board et al. (1979), 24 O.R. (2d) 279, 97 D.L.R. (3d) 304, 46 C.C.C. (2d) 342. This decision is now under appeal to the Ontario Court of Appeal, where the constitutional issue, discussed only in the dissenting reasons for judgment of O'Driscoll, J., will likely be a principal concern. In the Divisional Court the majority, Grange and Southey, JJ., expressed no opinion on the constitutional validity of the provincial legislation purporting to authorize the creation of the Board because they felt that the issue had not been raised in argument. Mr. Justice O'Driscoll, on the other hand, found the existence of the issue in a statement in one of the factums. It was his view that section 31 of The Mental Health Act was rendered inoperative by the enactment of what is now section 547 of the Criminal Code. His view was expressed, it should be pointed out, in the context of a discussion of the proper court before which a motion for judicial review of a decision of the Advisory Review Board (more properly, a recommendation) should be brought. It was his opinion that the Divisional Court had no jurisdiction because the Board must be a "federal board, commission or other tribunal" and, consequently, only the Federal Court of Appeal had the jurisdiction to review its decisions (see the reasons of O'Driscoll, J., at pp. 286-287 O.R.). Although the majority did not agree with the reasoning of Mr. Justice O'Driscoll, with respect to the jurisdiction of the Divisional Court, as opposed to the Federal Court of Appeal, it is not difficult to draw an inference from the reasons of Mr. Justice Grange that if it were necessary to decide the matter, he might not disagree that section 31 of The Mental Health Act became inoperative with the enactment of section 547

of the Criminal Code. See his reasons at p. 296 (O.R.). That is the issue that I expect will be decided by the Court of Appeal. In the meantime, there is uncertainty, but for the purpose of what follows I shall assume that section 31 of The Mental Health Act is operative and move to the practice of the Advisory Review Board.

Before I do so, another digression is in order for the sake of completeness. I have already pointed out some of the differences that exist among the provinces that have Review Boards. With respect to those provinces whose Boards were created, and operate, under the provisions of the Criminal Code, those that report to their respective Cabinets, that is, those in which "Lieutenant Governor" is, in practice, interpreted as "Lieutenant Governor-in-Council", may not be the subject of judicial review by the Federal Court of Appeal. This is the result of the decision of that Court in Lingley v. New Brunswick Board of Review, [1976] 1 F.C. 98, which holds that since the decision of the New Brunswick Board of Review (created under the Criminal Code) is advisory only and not binding on the Lieutenant Governor, it is not one required to be made on a judicial or quasi-judicial basis and is therefore not reviewable. There is some difficulty in reconciling the view expressed in the dissenting reasons for judgment of Mr. Justice O'Driscoll in the Abel case (and, for that matter, the views of the majority also) with those of the unanimous Federal Court of Appeal in the Lingley case, not on the issue of the effect of the federal legislation on the validity of the earlier Ontario legislation, but rather on that of the reviewability of the decision of the Board if it is a federal board or tribunal. Finally, one wonders what applicability the reasoning in the Lingley case has with respect to those Boards, e.g., those of Quebec and Alberta, which do not report to Cabinet but have their decisions accepted, without question, as a matter of practice, by the Lieutenant Governor directly.

As I have indicated, in its reviews the Board has before it the hospital's files on the subject patients. It seems to me that, with the amendment of The Mental Health Act by the Ontario Legislature in 1978, its right to continue this practice is questionable, although, as yet, no one has challenged it. Before I explain why my doubt exists let me refer to a description of the Board's procedure, written by its chairman before the 1978 amendment, and applicable at least until the decision of the Divisional Court in the Abel case:

The procedure for review is as follows:

1. A date is set for the review and the patient and his lawyer are notified.

2. Within a few weeks of the review the two psychiatric members of the Board attend at the hospital and independently examine the patient, review his file and confer with the staff. Each psychiatrist makes a provisional summary.

3. If the patient wants his own psychiatrist to examine him, he is encouraged. Legal Aid often provides the fees for the psychiatrist. It also provides the fees for the lawyer.

4. If the particular lawyer wants to talk to the Administrator or doctors in charge, that is permitted. He may see the file in the discretion of the Administrator who will make such disclosure as the Medical Director or Superintendent deems advisable. See section 17 of The Mental Health Act. Here you must recognize that the situation can be very delicate. Many things entered in the file are confidential, or are disclosures made by others including patients. If these were disclosed it could be utterly destructive of the therapeutic community. While some of the facilities may look like jails you will soon learn that they are hospitals. There is no prison subculture. There are no guards, only nursing attendants. Many of them are highly intelligent and trained men and women. Occasionally you will encounter a suspicious lawyer or a paranoid patient who can be quite demanding about the file. Over the years, I have encountered no difficulties that could not be satisfied by reasonable discussion.

I have always made it clear that while as chairman of the Board The Mental Health Act permits me to demand the patient's file and use it for Board purposes, I have no power to command the psychiatric facility to produce it to a third party.

5. The hearing. In preparation for the hearing the Administrator of the facility has prepared a summary of the file and has the attending doctors on call.

Because of the large numbers at Penetang, a substantial casebook is prepared and is brought up to date for each hearing. The hearing commences by the Board reviewing the summary and exchanging views amongst themselves. The patient's solicitor is then invited into the room without the patient and I carefully explain to him -

- (a) that this is not an adversary proceeding but an inquiry in which we are seeking to recommend to the Lieutenant Governor in Council what is best for the patient and the public. The solicitor is encouraged to speak freely and often is told that we want to make him part of the solution. He is told that we desire to hear from the patient and intend to do so but that he is privileged to address us in the absence of the patient and call evidence. Informality and the seeking of the truth is the hallmark. There is no talk of onus. The entire discussion surrounds the question of an appropriate recommendation. Witnesses often come from great distances and are heard courteously and, if possible, in the presence of the patient. This should be encouraged because the patient's family then get a much clearer picture of the mental illness, often learning things the patient has withheld from them. Occasionally the patient's psychiatrist will ask to express his views in the absence of the patient, but in the presence of the lawyer. At other times the lawyer will present a medical report and other documents.
- (b) Frequently the lawyer will ask the patient to retire at the end of the hearing so that he may address us in the patient's absence. We usually permit this, but if in doubt, obtain the

patient's consent. We conclude this part of the hearing by thanking the patient, his lawyer and witnesses and telling them we will consider our recommendations. Sometimes they ask what we are going to recommend, and we tell them that we cannot make disclosure of this for the simple reason that our position is advisory only and what we advise may not be accepted by the Lieutenant Governor in Council. However, in due course, they will hear from the Lieutenant Governor.

- (c) Finally the Board goes into camera and considers the recommendations. The majority of cases are for "no change" but where change is recommended the custodial care is carefully spelled out and the two psychiatrists on the Board are asked to make written reports which will be attached to the recommendation. Generally the recommendations are unanimous. There may be one dissent and this should be indicated. Of course, there cannot be more than one dissent because otherwise 4 out of 5 would not be concurring and the result would be "no change".

I draw particular attention to the chairman's statement that he had "always made it clear that while as chairman of the Board The Mental Health Act permits me to demand the patient's file and use it for Board purposes, I have no power to command the psychiatric facility to produce it to a third party." I do so because it seems to me that the chairman's power to demand the patient's file, on the one hand, and the absence of power to command the psychiatric facility to produce it to the patient or the patient's counsel, on the other hand, are both in doubt because of statutory change in the case of the former and the Abel decision and statutory change in the case of the latter.

Even in this period between the enactment of the repeal of section 29 of The Mental Health Act and the proclamation of that enactment, it is my view that there is serious doubt about the right of the Board or its chairman to command the production of the patient's file for the Board's examination because of the enactment in 1978 of the present section 26a. That important section reads as follows:



26a.(1) In this section,

(a) "clinical record" means the clinical record compiled in a psychiatric facility in respect of a patient, and includes a part of a clinical record;

(b) "patient" includes former patient, out-patient, and former out-patient.

(2) Except as provided in subsections 3 and 5, no person shall disclose, transmit or examine a clinical record.

(3) The officer in charge and the attending physician in the psychiatric facility in which a clinical record was prepared may examine the clinical record and the officer in charge may disclose or transmit the clinical record to or permit the examination of the clinical record by,

(a) where the patient has attained the age of majority and is mentally competent, any person with the consent of the patient;

(b) where the patient has not attained the age of majority or is not mentally competent, any person with the consent of the nearest relative of the patient;

(c) any person employed in or on the staff of the psychiatric facility for the purpose of assessing or treating or assisting in assessing or treating the patient;

(d) the chief executive officer of a health facility that is currently involved in the direct health care of the patient upon the written request of the chief executive officer to the officer in charge;

(e) with the consent of the patient or, where the patient has not attained

the age of majority or is not mentally competent, with the consent of the nearest relative of the patient or, where delay in obtaining the consent of either of them would endanger the life, a limb or a vital organ of the patient, without the consent of either of them, a person currently involved in the direct health care of the patient in a health facility;

- (f) a person for the purpose of research, academic pursuits or the compilation of statistical data.

- (4) Where a clinical record,

- (a) is transmitted or copied for use outside the psychiatric facility for the purpose of research, academic pursuits or the compilation of statistical data, the officer in charge shall remove from the part of the clinical record that is transmitted or from the copy, as the case may be, the name of and any means of identifying the patient; and

- (b) is disclosed to or examined by a person for the purpose of research, academic pursuits or the compilation of statistical data, the person shall not disclose the name of or any means of identifying the patient and shall not use or communicate the information or material in the clinical record for a purpose other than research, academic pursuits or the compilation of statistical data.

- (5) Subject to subsections 6 and 7, the officer in charge or a person designated in writing by the officer in charge shall disclose, transmit or permit the examination of a clinical record pursuant to a subpoena, order, direction, notice or similar requirement in respect of a matter in issue or that

may be in issue in a court of competent jurisdiction or under any Act.

(6) Where the disclosure, transmittal or examination of a clinical record is required by a subpoena, order, direction, notice or similar requirement in respect of a matter in issue or that may be in issue in a court of competent jurisdiction or under any Act and the attending physician states in writing that he is of the opinion that the disclosure, transmittal or examination of the clinical record or of a specified part of the clinical record,

(a) is likely to result in harm to the treatment or recovery of the patient; or

(b) is likely to result in,

(i) injury to the mental condition of a third person, or

(ii) bodily harm to a third person,

no person shall comply with the requirement with respect to the clinical record or the part of the clinical record specified by the attending physician except under an order of,

(c) the court before which the matter is or may be in issue; or

(d) where the disclosure, transmittal or examination is not required by a court, under an order of the Divisional Court,

made after a hearing from which the public is excluded and that is held on notice to the attending physician.

(7) On a hearing under subsection 6, the court or body shall consider whether or not the disclosure, transmittal or examination of the clinical record or the part of the

clinical record specified by the attending physician

(a) is likely to result in harm to the treatment or recovery of the patient; or

(b) is likely to result in,

(i) injury to the mental condition of a third person, or

(ii) bodily harm to a third person,

and for the purpose the court or body may examine the clinical record, and, if satisfied that such a result is likely, the court or body shall not order the disclosure, transmittal or examination unless satisfied that to do so is essential in the interest of justice.

(8) Where a clinical record is required pursuant to subsection 5 or 6, the clerk of the court or body in which the clinical record is admitted in evidence or, if not so admitted, the person to whom the clinical record is transmitted shall return the clinical record to the officer in charge forthwith after the determination of the matter in issue in respect of which the clinical record was required.

(9) No person shall disclose in an action or proceeding in any court or before any body any knowledge or information in respect of a patient obtained in the course of assessing or treating or assisting in assessing or treating the patient in a psychiatric facility or in the course of his employment in the psychiatric facility except,

(a) where the patient has attained the age of majority and is mentally competent, with the consent of the patient;

- (b) where the patient has not attained the age of majority or is not mentally competent, with the consent of the nearest relative of the patient; or
- (c) where the court or, in the case of a proceeding not before a court, the Divisional Court determines, after a hearing from which the public is excluded and that is held on notice to the patient or (where the patient has not attained the age of majority or is not mentally competent) the nearest relative of the patient, that the disclosure is essential in the interests of justice.

It will be seen that the qualification to subsection 2 does not include the purposes of the Advisory Review Board. It may well be that a court would interpret subsection 4 of section 29--the subsection requiring the officer in charge, for the purpose of an inquiry, to furnish the chairman with such information and reports as he requires--as referring to documents other than the "clinical record", in its use of the words "information and reports", because of the failure to make section 26a(2) subject to the provisions of section 29. It excepted only the provisions of subsections 3 and 5 of section 26a. Nor do I believe that subsection 5 of section 26a contemplated the handing over by the psychiatric facility to the Board or its chairman of the clinical record. At the very least it can surely be said that the current legislative arrangements are far from clear or satisfactory.

When one turns to the question of the Lieutenant-Governor's warrant patient's right to access to his or her hospital file, one encounters an even more complex problem. For, difficult as the issue of the determination of the current law may be, what the law ought to be is much more controversial. It will be recalled that the chairman of the Ontario Board was of the view that he had "no power to command the psychiatric facility to produce [the patient's file] to a third party." In the Abel case, the majority of the Divisional Court held that there does indeed exist a discretion to require that the file be made available to the patient's counsel. Thus, at pp. 295-296 (O.R.) Mr. Justice Grange had this to say:



One of the fundamental rules of natural justice is, of course, as put by de Smith at p. 178, "A party must have an adequate opportunity of knowing the case he has to meet, of answering it and of putting his own case." That is not however to say that the reports must necessarily be revealed. Normally he should be given the opportunity of perusal. One can readily imagine those reports containing allegations of fact detrimental to the applicant which could readily be refused. But there may be circumstances militating against full disclosure. As put by de Smith at p. 180 -

To the general rule there are various exceptions, some of which have already been indicated. There are cases where disclosure of evidential material might inflict serious harm on the person directly concerned (e.g. disclosure of a distressing medical report to a claimant for a social security benefit) or other persons, or where disclosure would be a breach of confidence or might be injurious to the public interest (e.g. because it would involve the revelation of official secrets, inhibit frankness of comment and the detection of crime, and might make it impossible to obtain certain classes of essential information at all in the future). In such situations the person claiming to be aggrieved should nevertheless be adequately apprised of the case he has to answer, subject to the need for withholding details in order to protect other overriding interests.

There is no question that the exercise of the discretion to require the production of the reports might in this instance cause grievous harm to the administration of the Centre and indeed to the patient. But the problem as I see it is that the question was never faced. The Chairman denied the request for production upon the ground that he

had no jurisdiction. No doubt he meant that he had no jurisdiction to order the Medical Centre to produce the files; he needed no jurisdiction to hand over to the applicants' counsel the reports which the Board had received pursuant to s. 29(4) of the Mental Health Act. What was needed, in my respectful opinion, was consideration of whether or not those reports should be disclosed to the applicants. When the Chairman failed to consider that question and answer it according to proper principles there was a failure of natural justice.

But, even apart from the decision of the Divisional Court and its fate in the pending appeal before the Court of Appeal, the provisions of section 26a of The Mental Health Act, as enacted in 1978 (assuming, again, that the provincial Legislature is competent to legislate in this field, and one can reasonably distinguish competence with respect to patient's rights, including rights of access to information, from competence with respect to the creation of a board of review), are surely relevant. Under the authority of subsection 3 of section 26a the clinical record may be examined by anyone (including, one presumes, the patient himself) with the permission of the officer in charge if the patient consents. If it should turn out that the Board may operate under the provincial Act, then, in the event of a refusal on the part of the officer in charge and the attending physician, the patient may be able to rely on the reasoning in Abel in asserting that the chairman of the Board has the power to compel the disclosure of the hospital records. On the other hand, if the Board must operate under the Criminal Code, then, by reference to the incorporated powers found in the Inquiries Act, a power to compel production exists, and the objection of the facility to that production may be the subject of the procedure provided for by subsection 6 of section 26a of The Mental Health Act, outlined above.

Whether the law ought to be changed to make it clear that a patient is entitled to access to his or her psychiatric hospital record is, as I have said, highly controversial and, in my view, a most difficult question. In addition to my own experience as alternate chairman of the Advisory Review Board, I have had the benefit of studying the conflicting interests or positions, expressed articulately by the Honourable Mr. Justice E.L. Haines, the chairman of the Advisory Review Board, on the one hand, and Dr. Jerry Cooper, a psychiatrist with extensive experience in forensic psychiatry on the other. Although the Advisory Review Board was ably represented at our policy hearings by Barry

Swadron, Q.C., the Board's secretary, the written brief filed was prepared by its chairman. In it, Mr. Justice Haines, in submitting that confidentiality of psychiatric records required that the records be kept secret, as against the patient, had this to say:

#### RECORDS:

This brings up an issue raised occasionally by some lawyers. While being told that in a psychiatric hospital for the treatment of the criminally insane their patient's record often contains the records of the conduct of other patients engaged in the ongoing therapy, that disclosure will destroy the confidentiality so essential to modern treatment, might damage the institution, and place third parties at serious risk of harm, nevertheless they persist in their requests to see the clinical record. Appendix "D" is a review of the problem of confidentiality prepared by the Medical Director of Oak Ridge, one of our most experienced psychiatrists with extensive experience in penal and psychiatric institutions. He speaks from a deep well of experience. If one were to pause here and read the Appendix he may see why confidentiality must be maintained. There comes a time when we must trust those men in charge to do what is best for the patient, the institution and society. In the context of the patient's entire treatment, it is essential that he feel confident in those engaged in his treatment and recovery. No doubt in his mind, the reviews by the Board are part of the system. If at all possible, he should not be engaged in an adversarial role concerning his hospital history and records. He should feel that fair disclosure is being made according to the competing interests and values. The present solution to this problem is a conference between the lawyer and a senior member of the institutional staff who reviews the records with the lawyer and makes such disclosure of those items to the lawyer as will assist the patient and not harm the institution or society. So much depends on the sound wisdom and integrity of the Bar in

interpreting the issues to the patient. Fortunately to date that has been sufficient.

Appendix "D", referred to in the passage quoted, is a letter to Mr. Justice Haines from Dr. Ronald E. Stokes, the Medical Director of Penetanguishene Mental Health Centre, dated October 4, 1979, and reads as follows:

10.04.79

The Honourable Mr. Justice E. Haines,  
The Supreme Court of Ontario,  
Osgoode Hall,  
Toronto, Ontario

Your Lordship:

I am responding to your request for comments regarding patient access to clinical records at the Oak Ridge Division of the Mental Health Centre, Penetanguishene. I appreciate that this matter has provoked concern regarding presentation of cases before the Advisory Review Board.

The practice of medicine including the specialty of psychiatry has been based on a conference paradigm. Consequently, information from a variety of sources is pooled, sorted, weighed and although assisting in the course of assessment and treatment, rarely is a single critical feature of the process. A clinical record may contain comments from terrorized family members, staff at other hospitals, employers, family physicians etc. The information is provided with the expectation that we shall deal with the information in a confidential manner. If we fail to do so, helpful data will cease to be available. Some jurisdictions, where provisions ensure the patient access to the clinical record, have developed a double record system with a secret record or correspondence file (not deemed part of the clinical record) that contains any third party information. Personally, I am opposed to such a procedure which I believe enhances the possibility of useful data being missed.

You may recall such a situation regarding a patient at another psychiatric hospital where a separate file was kept on the patient. It caused the Advisory Review Board much concern because the decision arrived at was modified when the file was finally made available.

It is necessary to recognize that such patients, sane or insane, constitute the most dangerous individuals in Ontario and often, hidden from our awareness, harbour resentment for an individual for many years. They have threatened staff, patients, family, judges and counsel, indeed there have been cases that have gone beyond threatening.

There are three persons I am concerned about having access to the clinical records of Oak Ridge patients: The patient's counsel, the patient and, and if incompetent, the next-of-kin. The counsel often believes that whatever is learned must be communicated to the client. It has been our experience that regardless of suggestion or admonition, many counsel reveal all to their clients. Mr. Jarvis, Secretary of the Law Society, suggested having disciplinary provisions enacted to ensure that lawyers, like physicians, must include respect of confidentiality as an ethical requirement; failure to comply could lead to disciplinary action by the governing professional body. With regard to next-of-kin, some clinical records may contain information from other members of the family or the patient that could promote serious disintegration or conflict in the family unit. This of course is contrary to our goal for most patients.

A unique problem arises on the Social Therapy Unit in the Oak Ridge Division. The very essence of the therapy programme involves considerable interaction with patient and peers. These interactions are observed and become a part of the recorded data on the clinical record. Thus, patient A may have information about patient B, C and D, on his clinical record. Those other



patients merit assurance that their observations are confidential or the system would fail and we have nothing else to offer this difficult group of patients.

In summary, we are dealing with an extremely dangerous group of individuals at the Oak Ridge Division. A distinction between counsel having access to the clinical record and the patient having access to the clinical record cannot be made. The clinical record contains third party information that would not be forthcoming unless we assured confidentiality to the third party. The clinical record may contain information about other patients. The observations signed by staff would not be available. Oak Ridge is not a popular facility to recruit staff for. If the clinical record were open to the patient, I do not believe the psychiatric staff would put signed notes on the record or probably would seek a more tranquil professional environment which currently is readily available to them.

Yours sincerely,

R.E. Stokes, M.D., D. Psych., F.R.C.P.(C).,  
Medical Director

I shall comment now on the written submission of the Advisory Review Board. Later I shall turn to the oral presentation made on its behalf. To begin with, I entirely reject any approach to these difficult questions that characterizes persons detained under the authority of a warrant of the Lieutenant Governor as criminally insane. They are not criminals for, in the case of those found not guilty on account of insanity, they have been acquitted of the offence or offences with which they were charged and, in the case of those found unfit to stand trial, they are simply accused persons for they have not yet been tried. These persons are mentally ill men and women who entered the system of mental health care because, in one way or another, their conduct brought them into contact with the criminal law enforcement authorities. It is true that they can, as I shall have occasion to point out later, be distinguished from other categories of mentally ill patients, even those who were involuntarily civilly committed to psychiatric facilities. But to begin a consideration of the solution to the hard

questions I have asked from the premise that patients detained in a psychiatric facility under Lieutenant Governor's warrants are criminally insane or persons who have committed crimes, is an error that will make the right solution more difficult.

I concede at once that there is judicial authority in Ontario, and strong judicial authority at that, for the proposition that one who has been found not guilty on account of insanity is a "criminally insane" person, has committed a crime and ought more accurately to be considered as guilty but insane. Statements to that effect can be found in the judgment of the Court of Appeal in Rex v. Trapnell (1910), 22 O.L.R. 219. That was a case in which the accused, who was an attendant at the Hamilton Hospital for the Insane, was charged with assisting the escape of two patients, both men who had been confined in the asylum in Hamilton in consequence of a finding that they were not guilty of murder, with which they had been charged, on account of insanity. The offence charged was a common law offence, (common law offences had not yet been abolished in Canada) but could not be made out unless it could be shown that the two patients, or either of them, had, before the escape, been confined in a prison. In holding that the accused had been properly convicted, Mr. Justice Meredith, for the Court, made certain statements about the status of a person who had been acquitted of an offence on account of insanity that are pertinent. They include the following remarks, found at pp. 222, 223 and 224:

But it is said that these men had been acquitted, and how, then, could they be detained except as lunatics simply? It is true that they were, in a sense, acquitted by the juries by which they were tried; but the acquittal was a part only of the verdicts; they were special verdicts under s.966 of the Criminal Code, the full import of which was that each had committed the crime with which he was charged, but was insane at the time, and on that ground only was acquitted... (pp. 222-3)

It, therefore, seems to me that these men were in custody under the criminal law of the Dominion by reason of the crimes which they had committed; and no one can doubt the power of Parliament to impose such a penalty even upon one who has the excuse of insanity for his misdeed;... (p. 223)

right cannot, in my opinion, be abridged by a mere rule of professional conduct made by the Law Society of Upper Canada. A statute, that is an Act of the Legislature, is required to affect so detrimentally such a substantial right of a member of the public who is a client of a lawyer. The same criticism may be directed at Recommendation 27 of the Legal Task Force of the Committee on Mental Health Services in Ontario. With respect to involuntary civil committal, the Task Force makes certain recommendations about access to information by a patient, a matter I shall deal with elsewhere in this report, and then goes on to say this about the power of the regional review board on the proposed Mental Health Review Board:

Rec. 27 THAT the review board be authorized to disclose confidential matter to counsel on a formal undertaking that it will not be discussed or information revealed to any other person, subject to any amendment being made, if necessary, to the Rules of Professional Conduct of the Law Society of Upper Canada recognizing the right of a solicitor to enter into such an undertaking and making it a matter of professional complaint to fail to honour it.

The letter from Dr. Stokes contains another point about which there is some confusion. The confusion is compounded by the failure to recognize that respect for confidentiality on the part of lawyers is already part of their code of ethics. Indeed it is only the lawyer-client relationship to which the law in Ontario extends protection. But that sort of confidentiality ought not to be confused with an obligation to keep information from the lawyers' clients. Dr. Stokes says that lawyers, like physicians, must learn to respect confidentiality. I have already dealt with the right of a client to insist on learning what his or her lawyer knows. I do not know of any obligation a physician may have to respect confidentiality in the sense of an ethical or legal obligation to keep his or her patient in ignorance where the patient wants to know. The key to the confusion, in my opinion, is that one is not concerned with confidentiality at all on this issue. What is involved is the right of a patient or client to access to information in the hands of his or her physician or lawyer. A fuller discussion of this problem is found elsewhere.

From a written submission and one extreme I turn to an oral submission and the other extreme. The point was made

during the appearance at our policy hearings of a delegation from the Ontario Medical Association. One of the members of that delegation, Dr. Jerry Cooper, a psychiatrist with considerable experience in forensic psychiatry, speaking entirely for himself, and with reference to patients' access generally, expressed the opinion, and expressed it forcefully, that it would be dangerous and foolhardy to give patients access to their records. When the subject turned to the Advisory Review Board, however, Dr. Cooper was equally adamant. His opinion was that the review involved a political decision and that it was important, in order to avoid the appearance of deciding questions about freedom of the individual behind closed doors, that the patients ought to have access to their files. In his words, "I think that really there is a lot of concern as to how the review board makes its decision."

It will be recalled that under the practice that has developed in Ontario the two psychiatrist members of the Board make an examination of the patient before the review is held. Normally these Board members make notes of their examination or interview and these notes form the basis of participation in the Board's deliberations after the evidence and submissions have been heard and the parties retire from the hearing room. Earlier I quoted from a letter from a patient's counsel requesting "disclosure of all written or oral information made available to any or all members of the Board prior to or during Mr. 's hearing." It can be expected that requests of this sort will be made with increasing frequency. In my view, a distinction can be made between access to the clinical record and reports prepared by the facilities' psychiatrists, on the one hand, and the notes made by the psychiatrist Board members, on the other hand. The latter, it can reasonably be argued, are simply an aid to memory to be resorted to when the Board is in executive session and there is surely some justification for the position that the Board's deliberations, including the expression of views of its members while deliberating, are confidential and need not be disclosed except to the extent that they may appear, either expressly or implicitly, in the Board's report to the Lieutenant Governor in Council. In any event, since the decision in the Abel case, the chairman of the Board has developed a practice which is described in the following typical ruling:

RULING WHEN PATIENT OR HIS LAWYER DESIRES TO  
SEE THE NOTES OF MEMBERS OF THE ADVISORY  
REVIEW BOARD:

The Advisory Review Board is an independent body composed of a Supreme Court Judge as

chairman, two psychiatrists not of the facility where the patient is kept, a lawyer and a layman. They are charged with the duty of reviewing the case of the patient and advising the Lieutenant Governor as to whether the patient has recovered and as to whether in its opinion it is in the interest of the public and the patient that he be discharged absolutely or subject to conditions. The review embraces both medical and public consideration. Four of the five members must agree in order to make a recommendation. The Mental Health Act provides that any member of the Advisory Review Board may interview the patient or other person in private.

The Psychiatric members of the Board do not want to form an opinion on the mental health of the patient without first examining him. It makes much more adequate review and reduces the margin of error in ascertaining the degree of recovery, the prediction of dangerousness and the recommendation of suitable controls.

It is the practice of the psychiatric members of the Advisory Review Board to interview the patient in private so that along with the other members of the Advisory Review Board they may perform their duties. The same right of interview applies to all other members of the Board. Because there are many cases to review, its members make such notes as they deem appropriate to enable them to discuss the case during the review. These notes are in such form as the maker sees fit. They are much the same as any judge or other professional would make on reviewing a case in which he is about to participate. They may record preliminary impressions. They are an aid to the memory. They are for the use of the maker. To produce them would be unfair to both the maker and to an adequate review.

It is the view of the Chairman that the notes of any member of the Advisory Review Board should not be made available to the



patient or his lawyer. They are for the assistance of the members only and are shared, amplified and amended as the review proceeds.

These notes are not to be confused when the Chairman requests the psychiatrist or any member of the Advisory Review to express his final conclusions in writing for the assistance of the Lieutenant Governor in Council. They become part of the Board's recommendation.

*Recommendation:*

86. *That the notes made by the psychiatrist members of the Advisory Review Board and any other members who, before the review, interview the patient, intended for use in the deliberations conducted in the executive session of the Board, be protected from disclosure to the patient or his or her counsel unless the Board, in its discretion, decides otherwise.*

The two questions, the answers to which I described earlier as unclear, relate to the right of the Advisory Review Board to inspect the clinical record and to the right of the patient or his or her counsel to inspect it. Inspection by the Board, a practice in Ontario, as I have shown, is not uniformly resorted to by the Boards of Review across Canada. The practice varies from province to province. The schedule to this chapter is a survey of the practices in the seven other provinces with Review Boards for patients detained under a warrant of the Lieutenant Governor. With respect to Ontario, I agree with the view of the Legal Task Force to the Committee on Mental Health Services in Ontario on the subject of access to the clinical record by the regional boards of review or the proposed Mental Health Review Board and would apply the same reasoning to the Advisory Review Board. To function efficiently it should have access to any information it considers important that may be in the hands of the psychiatric facility in which the patient being reviewed may be detained, including that patient's clinical record.

*Recommendation:*

87. *That The Mental Health Act be amended to make it clear that the Advisory Review*

*Board, for the purposes of its review of the cases of patients detained under the authority of a Lieutenant Governor's warrant, has the right to inspect any information in the hands of the psychiatric facilities in which the patients are detained, including the patients' clinical records.*

Access to the clinical record by the patient or his or her lawyer is much more difficult. I reject as unsatisfactory and unacceptable the two extreme positions which I have summarized above. On the other hand, I accept without question the description given by Dr. Stokes of some of the patients detained under warrants of the Lieutenant Governor as dangerous. They may be distinguished from other categories of mentally ill persons in whom there may be no propensity for violence or in respect of whom it may be difficult to predict dangerous behaviour. Most of these patients have some history of serious anti-social conduct, usually of a violent nature. One cannot be permitted, however, to second guess the decision that these persons, by whatever means they came to the attention of the authorities, are or were seriously mentally ill; they have been so found by a court of competent jurisdiction. They have accordingly been deprived of their liberty. Fairness and fundamental concepts of justice demand that persons involuntarily kept in custody shall have their deprivation of freedom adjudicated upon from time to time. This is the reason for the very creation of the Advisory Review Board. As was pointed out in the Abel case, the Board must govern itself in a way that is fair to the patient. There would be no fairness if the patient or the lawyer he or she is entitled to have represent him or her were denied the opportunity of learning what facts or evidence the Board has that will form the basis of its decision and that might result in a "no change" recommendation. But, again, owing to the nature of a psychiatric record and the nature of the patients' conditions, there are cases, a minority according to the evidence, to be sure, in which, in the interests of the patients or third parties, denial of access to the record might be justifiable. Because cases of this sort are, according to the evidence, the exception rather than the rule, the general principle ought to favour access, not secrecy. The exception, that is, refusal of access, should be the subject of some appeal mechanism and for this reason cases falling within the exception should be dealt with in accordance with the recommendation, found elsewhere in this report, respecting access to one's own health information and, for that matter, with the principle underlying section 26a of The Mental Health Act and, finally, the recommendations of the Legal Task Force of the Committee on

Mental Health Services in Ontario. Nor is this resolution inconsistent with the submission of the Advisory Review Board as presented orally at our policy hearings by its secretary, Barry Swadron, Q.C. At the hearing, after a thorough discussion of the problem faced by the Board, Mr. Swadron very fairly stated the case for the Board. After pointing out that the cases in which full access would be harmful to the patient or a third person amounted to a small fraction of the Board's entire case load of approximately 270, Mr. Swadron engaged in the following exchange with Mr. Strosberg:

MR. STROSBURG: Could I just ask you this? The last question, I promise. Are you saying then that there should be a prima facie right to access, subject to someone at the administration in the hospital coming along to the board and saying all right, this portion ought not to be disclosed?

MR. SWADRON: Something like that. Either the administration or the board. It might be that the administration will say, here, you have it, and then it's not a matter for the board because they have got it all anyway.

MR. STROSBURG: All right. But it's a prima facie right subject to someone convincing the board.

MR. SWADRON: Absolutely. Absolutely. If there is no reason for refusal of disclosure, there is no contest. The patient or his legal representative should have total access if there is no reason that it should be refused in part.

The mechanism recommended in the general discussion of patient access is, in my view, entirely capable of meeting the needs and concerns of the Advisory Review Board as so ably expressed by Mr. Swadron in his appearance at our hearings.

*Recommendation:*

*88. That The Mental Health Act be amended to express the general rule that, for the purpose of a hearing before the Advisory Review Board, the patient or his or her counsel has a right to inspect the patient's clinical*

*record. If the administrator of the psychiatric facility to which the patient is related is of the opinion that, in the interest of the patient's treatment, recovery, health or safety, or the health or safety of another person, access to the clinical record ought to be denied, that issue should be decided by the Chairman of the Advisory Review Board, whose decision should be subject to review by the Divisional Court or a judge of that Court.*

Another matter deserving discussion relates, not to the confidentiality of psychiatric records and the Advisory Review Board, but to information about the outcome of the recommendations of the Advisory Review Board in the form of Cabinet decisions respecting patients under warrants of the Lieutenant Governor. The decisions themselves, under my terms of reference, are none of my concern but publicity attending these Cabinet decisions (or the absence of publicity) does raise the question of confidentiality for two reasons. First, the subjects of the decisions are patients who were, and perhaps still are, mentally ill and, second, one of the criteria by which the Advisory Review Board arrives at its recommendation, in the case of a person found not guilty on account of insanity, it will be remembered, is whether "that person has recovered."

On at least one occasion in the recent past, the public in Toronto became alarmed upon learning through press reports that a Lieutenant Governor's warrant patient had been permitted to leave hospital to spend time in the community under a modified, or, as it is unfortunately termed, a "loosened" warrant of the Lieutenant Governor. The conflict of interests involved is that of the public's perception of danger and its concern for safety, on the one hand, and the patient's entitlement to privacy and concern for the confidentiality of his or her health information, on the other. In this connection, there is, of course, one obvious difference between Lieutenant Governor's warrant patients and other mentally ill patients and that is the public nature of the process of committal to a psychiatric facility of the former. That difference, in my opinion, however, does not dictate that, after the committal, the Lieutenant Governor's warrant patient should be denied the privacy that all other involuntarily committed patients are entitled to. Once the judicial order of committal is made, the person who is the subject of the order should be treated as a patient and nothing affecting his or her health information should turn on the means by which he or she became a patient.

Experience and a concern for common humanity justifies the view that members of the public should have, or should learn to have, faith or confidence in the Lieutenant Governor's warrant system, faith or confidence, that is, that, to the extent that these matters can be predicted by fallible human beings, dangerous persons will not be released into society. Again, no recommendation for greater freedom for the patient can be made unless the Advisory Review Board is of the opinion that the person has recovered. The involvement of the Cabinet, a politically responsible and sensitive body, is an additional safeguard. There will, of course, always be a risk, a very small risk, one hopes, that a mistake will be made and that a patient released from strict custody will commit a socially harmful act. That is a risk that an enlightened and humane society will run. The alternatives are worse. The first is that these patients should spend the rest of their lives under strict security, whether or not they have recovered and whether or not it is in their interest and in the interest of society that they be discharged, surely an unacceptable solution. The second is that the community, including the police, should be alerted whenever one of these patients is accorded more freedom in society, a measure that would amount to harassment of persons who committed an anti-social act because they were sick, surely an equally unacceptable solution.

*Recommendation:*

- 89. That the recommendations of the Advisory Review Board and the subsequent decisions of the Cabinet be treated confidentially and not be made available for public access.*

APPENDIX

SURVEY OF THE PRACTICES OF THE  
OTHER SEVEN PROVINCIAL REVIEW BOARDS

This survey reflects the answer given by the chairmen of the Review Boards in Canada to the following questions:

- (1) Is there disclosure of the hospital records, which the Board sees during or before a review of a patient's case to the patient or his counsel?



- (2) If there is no automatic disclosure of the records, will they be disclosed if a request to be permitted to inspect them is made?
- (3) Do patients have a right to be represented by counsel?
- (4) If so, do patients exercise the right?
- (5) Are counsel ever shown the records upon the express undertaking that they will not reveal their contents to their clients?
- (6) Are patients permitted to be present during the review?
- (7) May patients be excluded when some of the testimony is heard?

#### British Columbia

- (1) There is no automatic disclosure but see the answer to question 2.
- (2) On request, counsel is given access to psychiatric reports prepared by the Forensic Psychiatric Services but they are not provided with nursing notes. Psychiatric reports are not given directly to patients. A patient's private psychiatrist is given full access to the hospital files for the purpose of assessing the patient and giving his opinion.
- (3) Patients have the right to legal representation and are so advised prior to the review.
- (4) Patients exercise this right in only 5-10% of the cases. From April 1977 to April 1979, of 391 reviews patients were represented in only 25 reviews of which 11 were of a repeat nature.
- (5) Apparently no undertaking is required of counsel.

- (6) Patients are always present at the review, and only in exceptional cases, where it would be in their best interest, are discussions held with treatment staff out of their presence.
- (7) See the answer to question 6. Viva voce evidence is not heard. Written reports of the forensic psychiatrists are given to the Board which also has access to the entire hospital file.

### Alberta

- (1) The Board itself does not request access to the actual hospital records and these records are not physically examined by the Board or by counsel. The Board receives copies of case conference reports and is given information from the hospital records by the psychiatrist. Psychiatrists' reports are provided to the Board prior to the hearing and these are also forwarded to the patient and counsel.
- (2) See the answer to question 1.
- (3) Patients may be represented by counsel.
- (4) Patients nearly always exercise this right.
- (5) See the answer to question 7.
- (6) Patients are generally permitted to be present throughout the hearing.
- (7) The Board may exclude the patient from the hearing. This would only be done if the Board were convinced, on the basis of medical evidence, that it would be detrimental to the health of the patient to be informed of certain aspects of his condition. This applies equally to written psychiatric reports and the psychiatrists' oral reports to the Board. If it is necessary to exclude the

patient from the hearing, his counsel is permitted to remain upon undertaking not to disclose the detrimental information to the patient.

Saskatchewan L.G.W. patients other than the mentally retarded, who are very few in number.

- (1) There is no automatic disclosure but see the answer to question 2. The entire medical record of the patient is in the board room and available for examination by members of the Board of Review while it is meeting.
- (2) Counsel is given a summary prepared by the staff of the facility, the same summary that the Board members are given. Counsel is allowed free access to all medical records but is asked not to allow the patient to see his own record. A request by counsel to examine a portion of the record during a Board hearing has never been refused.
- (3) Patients are entitled to be represented by counsel.
- (4) Patients exercise the right to be represented.
- (5) See the answer to question 2. There has been only one instance in which a patient was shown the record by his counsel and that episode caused considerable trouble to the staff.
- (6) The patient is permitted to be present during the review, except when the Board is deliberating. Where a patient has counsel it is left to counsel to decide whether he or she wishes the patient to be present throughout and counsel will be heard in the absence of the patient if counsel so requests. Members of the medical staff are not present but are available, and will appear at the

Board's request or if counsel desires to question them.

- (7) Patients may be excluded at the request of their counsel.

### Manitoba

- (1) There is no automatic disclosure of hospital records to the Board of Review but they will be disclosed if the request is made. This is seldom, if ever, done. The Board requests and receives up-to-date medical reports on patients regularly and these reports contain information from the hospital records.
- (2) Counsel appear to obtain information about their clients directly from their patients' physicians and not from or through the Board.
- (3) Patients are entitled to be represented by counsel.
- (4) The Board reviews the case of each and every patient (approximately 25 in number) monthly. In the last 7 or 8 months there have only been two or three specific hearings convened at the request of the Board itself or a patient and on two occasions counsel have appeared with the patient.
- (5) See the answer to question 2.
- (6) Patients are permitted to be present during the review.
- (7) The Board does, in some instances, exclude the patient when conducting the inquiry which is conducted informally without sworn evidence. The "evidence" is not transcribed.

## Quebec

- (1) Under the Health and Social Services Act the medical records are confidential but a patient who is refused access is entitled to apply to a court for an order granting access. The court is required to grant access unless it is "of the opinion that it would be seriously prejudicial to the health of the patient to examine his record."
- (2) The Board does not hesitate to disclose the gist of the medical reports if that is necessary.
- (3) Patients always have the right to be represented by counsel who may be present throughout, even when the treating physician is being heard in the absence of the patient.
- (4) Few patients exercise the right to be represented by counsel. Sometimes patients ask that a member of the family be present and that is always permitted.
- (5) Lawyers always have access to their clients' files and the Board trusts them on the question of disclosure of the contents.
- (6) The presence of the patient is not only permitted but is required. If the patient refuses to attend the Board confines itself to verification of medical reports and hears the treating physician.
- (7) As a general rule the treating physician is heard in the absence of the patient. However, he is present when the patient is heard and the patient is then free to question him.



## New Brunswick

- (1) The Board has full access to the hospital records for the purpose of a review but they are not made available to the patient.
- (2) Whether the hospital records would be disclosed to counsel is a decision of the hospital authorities who are loath to do so. The Board would not order the hospital authorities to do so, assuming it had the necessary authority.
- (3) Patients have the right to be represented by counsel but counsel would be advised that the hearing is not adversarial in nature. Full cross-examination of the expert witnesses is not permitted but is restricted to clarification.
- (4) Very few patients exercise the right to be represented. In the few instances which have occurred there has been good co-operation between counsel and the Board. Counsel for the Justice Department has been permitted to attend.
- (5) Counsel would be given a copy of the report made by the attending psychiatrist for the Board showing diagnosis, behaviour, treatment, medication and re-assessment of diagnosis.
- (6) The patient is usually interviewed but is not permitted to be present during the remainder of the review.
- (7) See the answer to question 6. The patient's presence is thought to inhibit open discussion which might be discouraging to patients and destroy the relationship with the patient's therapists.

## Nova Scotia

There was no legislation in Nova Scotia regarding confidentiality of psychiatric hospital records until April 1, 1979, when the Hospitals Act was proclaimed. Those in charge of such records formulated policies similar to what is now provided by legislation. If a problem arose, which apparently was not too often, they sought legal advice and abided by it.

In any event, it is fair to observe that those associated with such records were very careful and strict regarding confidentiality. Patients themselves could not gain information. Several instances in recent years gained widespread publicity where discharged patients wanted access to files but could not get it. The Freedom of Information Act appears to overcome this.

Section 63 of the Hospitals Act deals with confidentiality of hospital records in all hospitals in Nova Scotia today.

The Hospitals Act, R.S.N.S. 1967, chapter 249, (as amended and proclaimed in force as of April 1, 1979) provides, in section 63, as follows:

63. (1) The records and particulars of a hospital concerning a person or patient in the hospital or a person or patient formerly in the hospital shall be confidential and shall not be made available to any person or agency except with the consent or authorization of the person or patient concerned.

(2) If a person or patient or former patient is not capable of giving consent in respect of his records and particulars then such consent may be given by the guardian of such person if there is a guardian and if there is no guardian by the spouse of such person and if there is no spouse by the next of kin of that person and if there is no next of kin with the consent of the Public Trustee.

(3) Notwithstanding subsections (1) and (2), a hospital or a qualified medical practitioner may refuse to make available information from the records or particulars of a person or patient if he has reasonable grounds to believe it would not be in the best interest of the patient to make available that information.

(4) If a hospital or a qualified medical practitioner refuses to make available the records and particulars of a person upon request by that person or upon authorization of that person or agency or upon authorization pursuant to subsection (2) then the person requesting the records and particulars or authorized to receive the same may make application to a county court judge and such judge shall in his discretion determine whether the records and particulars shall be made available and to what extent.

(5) Nothing in this Section prevents the records and particulars of a hospital concerning a person or patient in the hospital or a person or patient formerly in a hospital from being made available to

- (a) a person on the staff of the hospital for hospital or medical purposes;
  - (b) the qualified medical practitioner of the person concerned designated by the person as his physician;
  - (c) a person authorized by court order or subpoena;
  - (d) a person or agency otherwise authorized by law;
  - (e) the Minister or any person or agency designated or authorized by the Minister.
- (6) Nothing in this Section prevents

- (a) the publication of reports or statistical information relating to research or study which do not identify individuals or sources of information; or
- (b) the transfer of the records and particulars of a hospital from one hospital to another hospital; or
- (c) the furnishing by a hospital of such information from the records and particulars of a person or patient in the hospital or formerly in the hospital to a municipal official as may be required for the purpose of establishing settlement.

(7) Nothing contained herein prevents a hospital or a qualified medical practitioner from disclosing general information on the condition of a person or patient unless that person or patient directs otherwise.

The Freedom of Information Act, S.N.S. 1977, chapter 10, contains the following provisions:

2. In this Act,

- (a) "access" means either the opportunity to examine an original record or the provision of a copy, at the option of the government;
- (b) "applicant" means a person who makes a request pursuant to this Act;
- (c) "denial" means the refusal by a department to provide access to information, to correct a record or to make a notation on a record upon a request being made pursuant to this Act;
- (d) "department" means any department, board, commission, foundation, agency, association, or other body of persons, whether incorporated or

unincorporated, all the members of which, or all the members of the board of management or board of directors of which

(i) are appointed by an Act of the Legislature or by Order of Governor in Council; or

(ii) if not so appointed, in the discharge of their duties are public officers or servants of the Crown, or for the proper discharge of their duties are, directly or indirectly responsible for the Crown;

and "Government" has the same meaning;

(e) "Deputy Head" means the Deputy Minister or the senior administrative officer of a department;

(f) "information" means information in any form including information that is written, photographed, recorded or stored in any manner whatsoever and on file or in the possession or under the control of a department and includes personal information;

(g) "personal information" means information respecting a person's identity, residence, dependents, marital status, employment, borrowing and repayment history, income, assets and liabilities, credit worthiness, education, character, reputation, health, physical or personal characteristics or mode of living;

6. (1) A person in respect of whom personal information is contained in a file by a department may

(a) request that the information be corrected and amended;



- (b) request that the information contained in the file not be used or made available for any purpose other than the purpose for which it was provided without consent;
- (c) seek injunctive relief to correct or amend personal information on a file maintained by a department.

2. A department maintaining personal information files shall

- (a) not make the personal information contained therein available to another department or person for another purpose without the person's consent;
- (b) maintain the records that are necessary and lawful, as well as current and accurate, and disclose the existence of all data banks and files it maintains containing the personal information;
- (c) refrain from selling or renting a person's name or address for mailing list use without that person's permission;
- (d) permit a person to have access at all reasonable times to the personal information respecting him contained in his file.









